Defense Manpower Data Center (DMDC)

Trusted Associate Sponsorship System (TASS)

Overview Guide

(TASS Overview Guide)

Version 5.03 **(EMMA Changes Only)**
June 2014

Prepared by:
The Defense Manpower Data Center

Document History

Version	Date	Author	Comments
5.00	05/23/13	DMDC	Original
5.03	05/22/14	DMDC	Updated current through TASS version 5.03 (EMMA changes only)

Table of Contents

1 Introduction

This Overview Guide includes a description of the Trusted Associate Sponsorship System (TASS) application. This section discusses the purpose and background of the Common Access Card (CAC) program.

1.1 Purpose of TASS

The TASS application, initially designed in 2003 as the Contractor Verification System (CVS), was designed to automate the paper application process using DD Form 1172-2, *Application for Department of Defense (DoD) CAC Defense Enrollment Eligibility Reporting System (DEERS) Enrollment*. See **Appendix A** and **Appendix B**, respectively, for copies of DD Form 1172-2 and instructions. As a web-based system, TASS allows the following populations to apply for a Common Access Card (CAC) or other governmental credential electronically through an approved DoD web application:

- Affiliated Volunteers (requiring DoD Network access)
- DoD and Uniformed Service Contractors
- Foreign Affiliates
- Non-DoD Civil Service Employees
- Non-DoD Presidential Appointees
- Non-Federal Agency Civilian Associates
- Non-US Non-Appropriated Fund (NAF) Employees
- OCONUS Hires
- Other Federal Agency Contractors

Government sponsors approve the applications to receive government credentials.

1.2 CAC Program Background

The DoD began issuing advanced identification (ID) cards for Active Duty Military, Selected Reserves, DoD civilians, and “inside the wall” Contractors in October 2000. The CAC is a personalized “Smart Card”—a plastic card the size of a credit card with an embedded integrated circuit chip (ICC) for storing and processing data. Incorporated with public key infrastructure (PKI) security, the CAC consolidates multiple types of credentials and data and may be used for various applications, including network security and secure email communication. For example, TASS supports various types of government credentials such as the Volunteer Logical Access credential and the Uniformed Services ID (USID) card.

The original CAC featured 32 kilobytes of Electronically Erasable Programmable Read-Only Memory (EEPROM) and supported on-card secure cryptographic functions, including key generation encryption and digital signing. With PKI, data encrypted with the public key may be decrypted only with the private key. The ICC contains protected data about the cardholder (including personal identification number [PIN]), personal demographics, benefits, digital certificates, and card management and security applets. Four unique digital certificates stored on the chip allow the cardholder to digitally sign documents, encrypt data for transmission or storage, and establish secure web sessions to access and update information via the Internet.

The new version of the CAC is equipped with 144 kilobytes of EEPROM. The increased memory provides for the creation of more complex and functional applets in support of business processes.

The Defense Manpower Data Center (DMDC) Identity Services Division and Identity Programs Branch Program Management and Development organizations sponsor the CAC program.

2 TASS Roles and Responsibilities

This section describes each of the roles within TASS and discusses the responsibilities of the individuals assigned to each role.

TASS users must meet the requirements listed in the following sections to assume their roles and responsibilities and qualify for access to the TASS application.

2.1 DoD Application

Since the release of version 2.0, organizations seeking to use TASS no longer need to submit a Memorandum of Agreement (MOA) to implement TASS service. The TASS application has become a DoD application and no longer requires every entity to possess an individual MOA with DMDC.

2.2 Defense Manpower Data Center (DMDC)

DMDC, as the administrator of DEERS and Real-Time Automated Personnel Identification System (RAPIDS), operates and maintains the TASS infrastructure. To manage the phases of the TASS Business Process, DMDC has created three TASS user roles, the Service or Agency Point of Contact (SPOC), the Trusted Agent Security Manager (TASM), and the Trusted Agent (TA). The TASS SPOC, TASM, or TA must fulfill with the responsibilities and comply with the position requirements listed for his or her role or the TASS role may be revoked.

Note: Applicants use TASS to submit applications for the government credential issuance process.

2.3 Service or Agency Point of Contact (SPOC)

SPOCs handle the day-to-day TASS management and operation. The TASS SPOC ensures that assigned TASMs and TAs meet TASS requirements. Therefore, they should be familiar with the requirements for each role. An SPOC fulfills the following key roles:

- Manages TASS for their service or agency
- Liaison between DMDC and other TASS roles
- Creates TASS sites
- Manages TASM registration and revocation
- Maintains other required field support

2.3.1 SPOC Responsibilities

An SPOC has the following responsibilities:

- Meet SPOC position requirements as specified in **Section 2.3.2 (SPOC Position Requirements)**
- Administer the TASS program within his or her service or agency, including establishing and updating Site ID numbers and Trusted Agent Security Manager (TASM) accounts

- Coordinate requests for new or additional TASS capabilities between his or her service or agency and DMDC
- Use the Enterprise Monitoring and Management of Accounts (EMMA) application to register and remove Site IDs and TASMs, and ensure the currency of site and TASM information
- Ensure that TASS TASMs and TAs complete all required TASS training, including both the TASS Certification Web-based Training (WBT) and the TASS training specified by the service or agency
- Transfer Applicants from an existing TASM/TA to another TASM/TA within the TASS application for his or her associated service or agency
- Create policies, operating procedures, and other supporting documentation in support of service- or agency-specific implementation
- Manage and oversee an internal Management Service that includes the following:
  - The service or agency TASS program
  - All responsible TASS sites
  - All responsible TASM accounts
  - Contact information for all TASM and TA personnel
- Ensure assigned TASM and TA personnel have met all requirements for their roles; see **Section 2.4.2 (TASM Position Requirements)** and **Section 2.5.2 (TA Position Requirements)**
- Provide documented policies and guidelines for assigned TASMs to provide training on how TAs are to complete and maintain the sponsorship process and their responsibilities

2.3.2 SPOC Position Requirements

The TASS SPOC must meet the following requirements:

- Be a U.S. citizen
- Be a DoD uniformed service member, DoD Civilian, or Contractor working for the service or agency
- Be a CAC holder
- Be capable of sending and receiving digitally signed and encrypted email
- Have a working knowledge of service or agency structure, including populations and missions of service or agency posts and sites
- Be familiar with PKI, the CAC issuance process, and the service or agency TASS Business Process policy
- Have not been convicted of a felony offense
- Have had a Federal Bureau of Investigation (FBI) fingerprint check with favorable results
- Have had, at minimum, a National Agency Check with Inquiries (NACI) background investigation performed
- Have completed the required annual TASS Certification Training
- Have not knowingly been denied a security clearance or had a security clearance revoked
- Be trustworthy

- Be retainable for a minimum of 12 months

2.4 Trusted Agent Security Manager (TASM)

The SPOC appoints TASMs for each site. Each site must have a minimum of two TASMs. Per DoDM 1000.13, TASMs should not manage more than 200 TAs without prior justification and approval from the SPOC. A TASM fulfills the following key roles:

- Administrates activities at their TASS site
- Manages users at their TASS site
- Oversees TAs at their TASS site

2.4.1 TASM Responsibilities

TASMs have the following responsibilities:

- Meet TASM position requirements as specified in **Section 2.4.2 (TASM Position Requirements)**.
- Act as a TA
- Troubleshoot TASS questions and issues for his or her site
- Manage TASM and TA users for his or her site
- Train an alternate site TASM and all TAs operating TASS
- Provide visibility for TASS at his or her site. The TASM may accomplish this via staff call, newsletter or weblink, or another effective means. Information should include the TASS location, hours of operation, telephone numbers, and other pertinent data
- Submit requests through his or her SPOC for new or additional TASS capability
- Coordinate all TASS matters with his or her SPOC
- Notify the SPOC and DMDC Support Center (DSC) of the following:
  - TASS outages
  - Suspected or known TASS system compromise
- Provision, appoint, or authorize TAs
- Ensure positive identification of all site TAs

Note: To access TASS and perform TASM duties, the TASM must pass the annual TASS Certification Training requirements; see **Section 3.9 (SPOC, TASM, and TA TASS Certification Training)**.

2.4.2 TASM Position Requirements

A TASM must meet the following requirements:

- Be a U.S. citizen
- Be a DoD uniformed service member or DoD Civilian working for the service or agency
- Be a CAC holder
- Be capable of sending and receiving digitally signed and encrypted email

- Have a working knowledge of the structure of the site under his or her control, including unit populations and missions
- Have had an FBI fingerprint check with favorable results
- Have had, at minimum, a NACI background investigation performed
- Have completed the required annual TASS Certification Training
- Have not been convicted of a felony offense
- Have not knowingly been denied a security clearance or had a security clearance revoked
- Not enrolled in TASS as a Contractor
- Be trustworthy
- Be retainable for a minimum of 12 months

Note: TASMs may not be Contractors. If a TASM who is also a Contractor attempts to log in to TASS as a TASM or TA, TASS will lock him or her out of the system and send an email notification to his or her SPOC, TASM, and TA.

2.5 Trusted Agent (TA)

A TA is a government sponsor to TASS Applicants who establishes the service or agency affiliation for registration of a government credential. TASMs identify and approve nominated TAs, and then register them in TASS through the EMMA application. DMDC policy (DoDM 1000.13) recommends that TASMs not exceed 200 TAs per site.

Note: Per DoDM 1000.13, TAs should not manage more than 100 active Applicants without prior SPOC justification and approval.

A TA fulfills the following key roles:

- Establishes sponsorship of the Applicant with the service or agency
- Verifies the Applicant's need for logical or physical access to either a DoD network or facility, both initially and ongoing through semiannual reverifications

Note: *Non-Federal Agency Civilian Associates* may not require logical or physical access to a DoD network or facility.

- Initiates the process of application for registration of a government credential

2.5.1 TA Responsibilities

TAs have the following responsibilities:

- Establish sponsorship of Applicants with the service or agency
- Notify the TASM or SPOC (if the TASM is unavailable) of site capability (TASS) outages
- Notify the TASM, SPOC, or DMDC Support Center (DSC) of any suspected or known TASS system compromise
- Be current with the TASS Certification Training requirement, which allows access to TASS to perform the duties of the TA role

2.5.2 TA Position Requirements

A TA must meet the following requirements:

- Be a U.S. citizen
- Be a DoD uniformed service member or DoD Civilian working for the service or agency
- Have had an FBI fingerprint check with favorable results
- Have had, at minimum, a NACI background investigation performed
- Be a CAC holder
- Be capable of sending and receiving digitally signed and encrypted email
- Have completed the required annual TASS Certification Training
- Have not been convicted of a felony offense
- Have not knowingly been denied a security clearance or had a security clearance revoked
- Not enrolled in TASS as a Contractor
- Be trustworthy

Note: TAs may not be Contractors. If a TA who is also a Contractor attempts to log in to TASS as a TA, TASS will lock him or her out of the system and send an email notification to his or her SPOC, TASM, and TA.

3 TASS Business Process Overview

The following sections describe the elements of the TASS Business Process. This section provides key steps necessary to operate TASS. Section 3.1 describes the process for creating TASS sites. Sections 3.2 – 3.7 explain guidelines for adding and training TASS users. The process for creating TASS applications is included in Sections 3.8 – 3.13. Finally, information on managing TASS records and revoking TASS sites and users can be found in Sections 3.14 – 3.18 and 3.19 – 3.20, respectively.

3.1 Site Creation

The SPOC starts the TASS Business Process by registering a site. A TASS site (sometimes referred to as a Site ID or Organization) is a logical collection of TASS users under the organizational control of a TASS TASM. Each TASM, in turn, reports to an SPOC.

The SPOC uses the EMMA application to register new TASS sites. To create a TASS Site ID, perform the following steps:

1. Access the Enterprise Monitoring and Management of Accounts (EMMA) application.
2. Click on the **SPOC (Project Officer Organization)** icon.
3. In the *Organization Details* section, select **Add Organization** from the drop-down menu.
4. Complete the fields on the *Add Organization* screen.
5. Click **Submit** to save the new Site ID (Organization) in EMMA.
6. Log out of the EMMA application.

Note: TASMs and TAs can find information about their site under the **My Profile** tab in TASS.

3.2 TASM Registration

After the TASS Site ID is created, SPOCs register TASMs for sites under their control. The following sections describe the process to register a TASM.

Note: Each TASS site must have a minimum of two TASMs.

3.3 TASM Registration Request

New TASM accounts are also registered through the EMMA application. In order to register a new TASM, the SPOC must have a valid email address for the candidate TASM. With this email information, the SPOC can log in to the EMMA application and complete the following steps:

1. Click on the **Site ID (Organization)** icon for the site that you wish to add the TASM to.

Note: Prior to adding individuals as TASMs for a new site, you **must** establish the TASM role. Once the TASM role has been established, you may skip to step 6 and begin the process of adding TASMs in EMMA.

2. In the *Organization Details* section, select **Add Role** from the drop-down menu.

3. Click **Go**.
4. Select a role to add from the *Select a Role* drop-down menu.
5. Click **Submit** to create a TASM role for the site.
6. On the left side of the screen, select the **TASM** role icon.
7. In the *Role Details* section, select **Add User** from the drop-down menu.
8. Click **Go**.
9. In the *Add User* window, type the 'Email Address' of the new TASM, the 'Number of Days' the TASM has to redeem his or her token, and click the **check box** to confirm the TASM's role.

Note: SPOCs should allow TASMs the maximum of 30 days to respond to the email to redeem their EMMA token.

10. Click **Submit**.
11. Log Off of the EMMA application.

Note: New TASM accounts are automatically created to include the TA role.

Important: TASS TASMs can NOT simultaneously serve in the role of RAPIDS operator.

3.4 TASM Registration Notification

When a new TASM is registered in EMMA, the TASM will receive an email notification prompting them to redeem their EMMA token. When the EMMA token is redeemed, the TASM’s TASS account is automatically activated.

Note: The TASM **must** redeem his or her EMMA token within the allotted time of 30 days. If the 30 day time frame has elapsed, the SPOC must log in to EMMA to provision the TASM again and generate another token email.

Important: A TASM can NOT be registered at more than one TASS Site ID.

TASS currently supports only one TASS Site ID per TASM. The TASM can be registered for more than one DMDC application if he or she serves in multiple roles (e.g., TASS, EMMA, CPR). Each DMDC application has a separate Site ID.

3.5 Updates to TASM Information

If a TASM requires an update to his or her information in the DEERS database (e.g., Name, Email, SSN), he or she should route these requests through the SPOC for verification. The TASM can then submit a separate request to the DMDC Support Office (DSO) with any required documentation. For example, a marriage certificate may be needed for a name change or a birth certificate for date of birth corrections. Allow at least 48 hours for DEERS changes to take effect.

Note: TASMs can use the RAPIDS Self-Service (RSS) portal (www.dmdc.osd.mil/self_service/) to make limited updates for DEERS data elements that do not require documentation (e.g., email address, home address, home telephone number, etc.). RSS changes will automatically be updated in DEERS.

3.6 TA Registration

When TASM is added to a TASS site, he or she is then able to identify and nominate TAs that meet the minimum qualifications established for the TA role; see **Section 2.5 (Trusted Agent)**. After verifying minimum qualifications, the TASM may approve and register new TAs to the TASS site under his or her control. Each TA, in turn, reports to a TASM.

Note: SPOCs and TASMs must ensure that a TA is not enrolled in TASS as a Contractor.

The TASM registers a TA in TASS through the EMMA application. A link to the EMMA application is also accessible in the TASS application for the TASM role only.

Note: For more information on using EMMA, access the *EMMA Quick Guide* under the **Resources** tab in TASS.

When the TASM registers a TA's account in EMMA, the TA will receive an email prompting them to redeem their EMMA token which will activate their TASS account. If the TA does not receive the email containing his or her EMMA token, he or she should contact the TASM who will resend the EMMA token email.

Note: TAs **must** redeem the EMMA token within the allotted time of 30 days. If the 30 day time frame has elapsed, the TASM must log in to EMMA to provision the TA again and generate another token email.

The TASM is the TA's primary point of contact (POC). If a TA's TASS account is in an inactive state, he or she will need to contact the TASM to have the account unlocked in EMMA. If the TA's **EMMA account** has been unlocked and he or she is still unable to log in to TASS, the TA's **DEERS account** may be inactive. To reactivate a TA's account in DEERS, the TA should complete the following steps:

1. Contact the DSC at 1-800-372-7437.
2. Provide the TASS error message received during the failed login attempt to the DSC representative.
3. Provide additional verification information to the DSC representative as requested.

The TASM should provide the TA with his or her Site ID and inform the TA to keep the Site ID on hand in the event that they need to contact the DSC for assistance with TASS Certification Training. The TA can be registered for more than one DMDC application if he or she serves in multiple roles (e.g., TASS, CPR). Each application has a separate Site ID.

Notes:

- TASS TAs can NOT simultaneously serve in the RAPIDS operator roles.
- For help with DEERS record corrections, either contact the DSO at 1-800-361-2508 or refer to the instructions for DEERS data changes in the TASS application.

3.7 SPOC, TASM, and TA TASS Certification Training

All new SPOCs, TASMs, and TAs must complete and pass the TASS Certification Training via the DMDC Learning Management System (LMS) prior to beginning their respective roles.

Note: SPOCs, TASMs, and TAs should follow the instructions in the *DMDC LMS User Guide* before logging into the DMDC LMS to ensure they have the correct system requirements to access and complete the training. The *DMDC LMS User Guide* is available in TASS under the **Resources** tab or on the LMS under the **Help Materials** link.

All active SPOCs, TASMs, and TAs must complete and pass TASS Certification Training on an annual basis. When the annual training date draws closer and the SPOCs, TASMs or TAs log in to the TASS application, they see a notification to complete the training requirement. SPOCs, TASMs and TAs receive the notification 30 days prior to the beginning of the 30-day recertification period. Once the 30-day notification has lapsed, SPOCs, TASMs, and TAs have 30 days to complete the certification training. If they do not meet the training requirement within 30 days, TASS locks them out of the application, preventing them from performing their duties within TASS until they satisfy the training requirement.

The SPOC must complete and pass the following training courseware on the DMDC Learning Site:

- TASS001, *Introduction to Web-based Training on the DMDC Learning Site*
- TASS002, *Trusted Associate Sponsorship System (TASS) Training Overview*
- TASS005, *Trusted Associate Sponsorship System (TASS) Service/Agency Point of Contact (SPOC) Training*
- EMMA 001, *Enterprise Monitoring and Management of Accounts (EMMA) Overview*
- EMMA 002, *Organization Functions in EMMA*
- EMMA 003, *Role and User Functions in EMMA*

The TASM must complete and pass the following training courseware on the DMDC Learning Site:

- TASS001, *Introduction to Web-based Training on the DMDC Learning Site*
- TASS002, *Trusted Associate Sponsorship System (TASS) Training Overview*
- TASS003, *Trusted Associate Sponsorship System (TASS) Trusted Agent (TA) Training*
- TASS004, *Trusted Associate Sponsorship System (TASS) Trusted Agent Security Manager (TASM) Training*
- EMMA 001, *Enterprise Monitoring and Management of Accounts (EMMA) Overview*
- EMMA 003, *Role and User Functions in EMMA*

Note: Site Security Manager (SSM) is a similar role in RAPIDS as that of a TASM role in TASS. In using the EMMA application or in completing certification training, TASMs may see the SSM role referenced, but should understand that in the context of TASS, the information applies to the TASM role.

The TA must complete and pass the following training courseware on the DMDC Learning Site:

- TASS001, *Introduction to Web-based Training on the DMDC Learning Site*
- TASS002, *Trusted Associate Sponsorship System (TASS) Training Overview*
- TASS003, *Trusted Associate Sponsorship System (TASS) Trusted Agent (TA) Training*

Successful completion of the training updates the SPOC, TASM, or TA's profile in DEERS. If TASMs and TAs do not successfully complete the training, the TASS application does not allow them to log in.

Important: A user is given five (5) attempts to pass a TASS certification course post-test. A failed fifth attempt locks them out of the course. To resume training, the user must call the DSC Help Desk at 1-800-372-7437 to have his or her test reset. Users can prevent lockout by considering the following tips:

1. Always read the course material thoroughly when navigating through the course.
2. Be sure to read the test questions and simulation instructions carefully before selecting an answer.
3. Allow the system time to process your action when taking a test that contains a simulation; refrain from clicking **twice** or clicking too fast while the simulation is in progress, or your simulation test will be graded as failed.
4. Press F5 to reload the simulation if it appears to stall while loading.

   Important: Each use of F5 will count against you as a failed attempt to complete the simulation. You have five (5) attempts to complete a simulation before lockout.

5. If the Internet connection is lost while taking the course, the system will automatically mark the post-test attempt that is in progress as failed. If Internet connection is lost, you will need to reestablish connection prior to resuming your test.
6. If the simulation inaccurately scores incorrect on the scored page of the simulation, be sure to properly exit out of the browser window to try again. DO NOT close the browser or the attempt will be marked as failed.
7. Press F11 when unable to see the simulation in its entirety. Select the browser window, and press F11 to resize it. This enables users to view the simulation in a larger window.

Note: Applicants have an option to complete the *TASS Overview WBT*, accessible within the TASS application under the **Resources** tab.

3.8 Applicant Requires Government Credential

Once the TASS Site ID exists and contains registered TASMs and TAs, Applicants can begin submitting requests for government credentials to their corresponding TAs.

The sponsoring DoD Agency provides the Applicant with the necessary information and appropriate paperwork required for obtaining a government credential.

The Applicant's employer then vets the Applicant using the DoD approved process. Once the Applicant, Contracting Agency, or Sponsoring Agency provide the necessary information, the Applicant submits the required information to the TA.

Note: A Contractor cannot be enrolled in TASS as a TASM or TA.

3.9 TA Submission of Application

Prior to the Applicant contacting a TA to request a government credential, he or she must first be vetted through his or her employer using the DoD-approved process and the process outlined in the following documents:

- Federal Information Processing Standards Publication 201-1, "Personal Identity Verification (PIV) of Federal Employees and Contractors"
- DoD Regulation 5200.2-R, "Personnel Security Program"
- Department of Defense Manual (DoDM) 1000.13, Volume 1—"DoD Identification (ID) Cards: ID Card Life-Cycle"

Notes:

- The TA should check with their service or agency for any additional internal policies or guidelines governing this process.
- All CAC holders must minimally have an initiated National Agency Check with Inquiries (NACI) and a favorable completion of an FBI fingerprint check, or a DoD-determined equivalent investigation, or greater. However, Affiliated Volunteers requiring network access are only required to have an initiated National Agency Check (NAC), and a favorable completion of an automated FBI National Criminal History Check (fingerprint check). Per policy, personnel (e.g., Non-Federal Agency Civilian Associates for National Guard State Employees and United Services Organization (USO) eligible only for the DD Form 2765 (self-sponsored Civilian ID card) do not require background vetting.
- The FBI fingerprint check adjudication process may take up to four weeks to complete. The TA must confirm the favorable completion of the FBI fingerprint check before he or she creates the application.

The TA must verify that the employer organization has vetted the Applicant according to these guidelines, and establish the affiliation of the Applicant with the service or agency. TASMs should check with their assigned TAs to ensure that the Applicant verification has been completed according to DoD and DMDC guidelines. Once the TA has confirmed the vetting, the TA creates the application for submittal.

Before a TA can create a new application, he or she must meet the following prerequisites:

- Ensure the Applicant is not registered as a TASS TASM or TA
- Determine and verify the Applicant has a valid requirement for a government credential
- Verify the Applicant's sponsoring service or agency has vetted the Applicant
- Have the following Applicant information:
  - Last Name
  - First Name

- Middle Name (optional)
- Person Identifier (e.g. Social Security Number [SSN])
- Email Address (use the Applicant's work email address, if available)
- Date of Birth
- Personnel Category
- Organization
- Eligibility Expiration Date
- Contract information (number and end date), if the Applicant is a DoD Contractor or Other Federal Agency Contractor

Note: TASS Applicants cannot be full-time Active Duty members. Applicants should consult with the TA if they hold a part-time Active Duty position.

3.10 Applicant Login

Once the TA submits a new application, the TA uses a secure means to provide the Applicant with his or her user ID and temporary password and the TASS weblink Uniform Resource Locator (URL). The Applicant can then log in to TASS to complete and submit the application. Once the TA submits the application, the Applicant has seven days to complete an initial log in to TASS and begin the application process, or TASS will automatically disable the application.

Once the Applicant has logged in for the first time, he or she has 30 days to complete the application process. The Applicant can save a partially completed application; however, the TA cannot process the application until the Applicant submits it in a complete form. Once the Applicant submits a completed application, the system automatically sends an email notification to the TA. The TA has 30 days to approve the application, otherwise the application automatically will disable. The Applicant cannot make changes to a submitted application unless the TA returns the application to the Applicant for correction.

Note: If the Applicant experiences TASS login issues, the Applicant should contact his or her TA for assistance with the TASS application. The TA can reset an Applicant's user ID or password, if required. An Applicant who cannot reach his or her TA should contact his or her employers to locate the TASS site TASM or SPOC for assistance.

3.11 Entering Previously Issued/Existing Credentials

An Applicant may possess valid credentials issued directly from a RAPIDS Issuing Facility and not through TASS. Applicants in this category, with the same sponsoring service organization, do not necessarily need a new credential. The TA can accept sponsorship of the existing credential through TASS and use the time remaining on the existing credential.

3.12 Verification

After the TA receives notification that the Applicant has submitted his or her application, the TA logs in to TASS and reviews the application. Upon review, the TA can reset the password, approve the application, return it to the Applicant for changes, reject, or disable it. Before approving an application, the TA must establish an Applicant's need for logical or physical access to either a DoD network or facility (may not be required for some Non-Federal Agency Civilian Associates), and verify vetting and the Applicant's affiliation with the service or agency.

Once the TA approves the application, the Applicant needs to obtain a card from a RAPIDS Issuing Facility within 90 days; otherwise, the system automatically disables the application.

If the TA rejects or disables the application, the system notifies the Applicant by email and updates the appropriate status in the Applicant record.

If the TA approves the application, the system updates DEERS with the Applicant information, and TASS reflects this status change in the Applicant record; see **Section 3.14 (DEERS Updates)**.

3.12.1 Letter of Authorization

Some Applicants require a Geneva Convention CAC due to the nature of their work. In accordance with the Department of Defense Instruction (DoDI) 3020.41, "Contractor Personnel Authorized to Accompany the U.S. Armed Forces," if the Applicant plans to work overseas, the Applicant may need to obtain a Synchronized Predeployment & Operational Tracker (SPOT) Letter of Authorization (LOA) and present it at the RAPIDS Issuing Facility, along with the other required identification and eligibility documents, in order to obtain the CAC. The requirement has expanded from an Army-only system to a Department of Defense (DoD)-wide system and is currently being implemented in other government agencies.

3.12.2 Status-of-Forces Agreement

Applicants who work overseas (e.g., those who accompany and support military forces) may require Geneva Convention CACs and may need to provide documentation of the appropriate Status-of-Forces Agreement (SOFA) at the RAPIDS Issuing Facility in order to receive a government credential.

SOFAs are usually an integral part of overall military base agreements that allow U.S. military forces to operate within a foreign host country. Each SOFA is negotiated separately with the individual host country and deals with particular circumstances unique to that country. SOFAs not only deal with issues necessary for day-to-day business, but also deal with civil and criminal jurisdiction. They are a means for the DoD to protect U.S. personnel who might be subject to foreign criminal investigation, prosecution, and imprisonment.

3.13 Card Issuance

Once the TA approves the application, the Applicant has 90 days to obtain a government credential from a RAPIDS Issuing Facility. To locate a RAPIDS Issuing Facility, Applicants can use the RAPIDS Site Locator (RSL) at http://www.dmdc.osd.mil/rsl/. The *Find Sites* details page on the RSL website includes information on making appointments. Some RAPIDS Issuing Facilities use an electronic appointment scheduler. In those cases, the Scheduling URL is listed on RSL *Find Sites* details page. At the RAPIDS Issuing Facility, an operator verifies and updates the DEERS data with the Applicant data and status of the card.

3.14 DEERS Updates

TASS runs a nightly offline process to provide DEERS updates to TASS regarding government credentials and card statuses. When the process runs after the RAPIDS Issuing Facility has issued a card, the TASS application status changes from 'Approved' to 'Issued.'

3.15 Applicant Reverification

Once Applicants have received a government credential, TASS requires the TA to either reverify or revoke active Applicant records every 6 months (180 days). In addition to confirming the Applicant's personal information and continued affiliation with the DoD for reverification, the TA must confirm that the Applicant has a continued need for a government credential. TASS notifies TAs and Applicants by email when reverification is due. A TA may also revoke an Applicant's government credential at any time. If the application is not reverified in 180 days, the application will be automatically revoked, which in turn will update DEERS and terminate the associated credential.

See **0** for the schedule for email notifications for Applicants requiring reverification.

3.16 Eligibility Expiration

Government credentials typically expire after 3 years. If a continued need for a government credential exists as the expiration date approaches, the Applicant must contact the TA and apply for a new credential.

Before the TA initiates the application process for a new credential, he or she must verify the Applicant's valid requirement for a new credential according to known policies and procedures, and the Applicant's continued employment or contract to the DoD.

3.17 Applicant Revocation

The TA can revoke an active TASS Applicant record at any time. The TA performs the revocation process within TASS by clicking the **Revoke** button on the *Reverifications-CACs for Reverification* screen. TASS simultaneously updates DEERS and terminates the personnel record, and DEERS subsequently terminates the card and updates the Certificate Authority (CA). The CA revokes the Applicant's certificates. The Applicant, TA, and TASM receive notice of the revocation by email. The TA coordinates the collection and return of the government credential in accordance with established policies, guidelines, and procedures. The TA must coordinate with Security personnel when Applicants do not return revoked cards.

Contractors must return the government credential to the issuing agency as soon as one of the following occurs, unless otherwise determined by the service or agency:

- When credential is no longer needed for contract performance
- Upon completion of employment
- Upon contract completion or termination

The contracting officer may delay final payment under the contract if the Applicant (Contractor) fails to comply with these requirements.

3.18 TA Sponsorship Transfer

A TASM can transfer Applicant sponsorship between TAs at their assigned site. An SPOC can transfer Applicant sponsorship between TAs for any site within their assigned service or agency. An SPOC or TASM might need to transfer sponsorship because the TA is sick, the TA no longer works in a TA capacity, or the TA has an unmanageable number of Applicants. SPOCs and TASMs use the TASS application to perform Applicant transfers. The system notifies the TASMs, TAs, and affected Applicants of the TA reassignments by email. Applicant transfer requests between two different services or agencies must be forwarded to the SPOC to coordinate the request appropriately with the TASS Program Office.

Note: DMDC policy (DoDM 1000.13) recommends that TAs not manage more than 100 active Applicants without prior SPOC justification and approval.

3.19 Site ID Removal

An SPOC may remove a TASS site for the following reasons:

- Service or Agency reorganization
- Site consolidation
- Site is compromised due to unauthorized access

To remove a TASS Site ID, the SPOC must log in to the EMMA application and complete the following steps:

1. Select the **Site ID** (Organization) that you want to remove.
2. In the *Organization Details* section, select **Remove Organization** from the drop-down menu.
3. Click **Go.**
4. In the *Remove Organization* pop-up window, click **OK**.
5. Log off of the EMMA application.

If the TASS Site ID being removed has active TASM, TA, or Applicant accounts, the SPOC must be sure to complete the following steps prior to removing the Site ID:

1. Ensure that you **transfer all active Applicant records** to another active TA at another site in TASS.

   Note: Each TA should manage no more than 100 active Applicants at his or her site. More than 100 active Applicants per TA must be justified and approved by the SPOC.

2. Ensure the **TASM removes all TA accounts** at the site from EMMA.

- If the TASM wants to reassign a TA account from one site to another, the TASM must first remove the TA account from their site. A new TASM can then add the TA to their site.

Notes:

- The TASM must coordinate with the SPOC to determine whether TAs assigned to a site should have their TA role removed or reassigned to another site.
- Each TASM should manage no more than 200 active TAs at his or her site. More than 200 active TAs per TASM must be justified and approved by the SPOC.

3. Use the EMMA application to **remove all active TASM/TA accounts** from the site.

   - If TASM/TA account(s) are still required, use EMMA to add the TASM/TA account(s) to an existing active site or to a newly created site.
   - When a TASM/TA account is removed in EMMA, the TA role is simultaneously removed. At times, a TASM may need to retain their TASS TA role. In this case, **the TASMs must log in to EMMA and create a duplicate TA account for themselves**. Once the TASM creates the duplicate TA account, the SPOC can log in to EMMA and remove the original TASM/TA account.

Note: Each site must have a minimum of two active TASMs.

3.20 Criteria and Actions for TASM Removal

An SPOC should immediately revoke a TASM's application and privileges if the TASM meets any of the following conditions:

- TASM is under investigation (or has been convicted) for any offense punishable by the Uniformed Code of Military Justice (UCMJ) or equivalent civilian law
- TASM has been relieved of duty
- TASM has left military service or civil service or has otherwise become disassociated with the service or agency
- TASM has transferred out of the organization

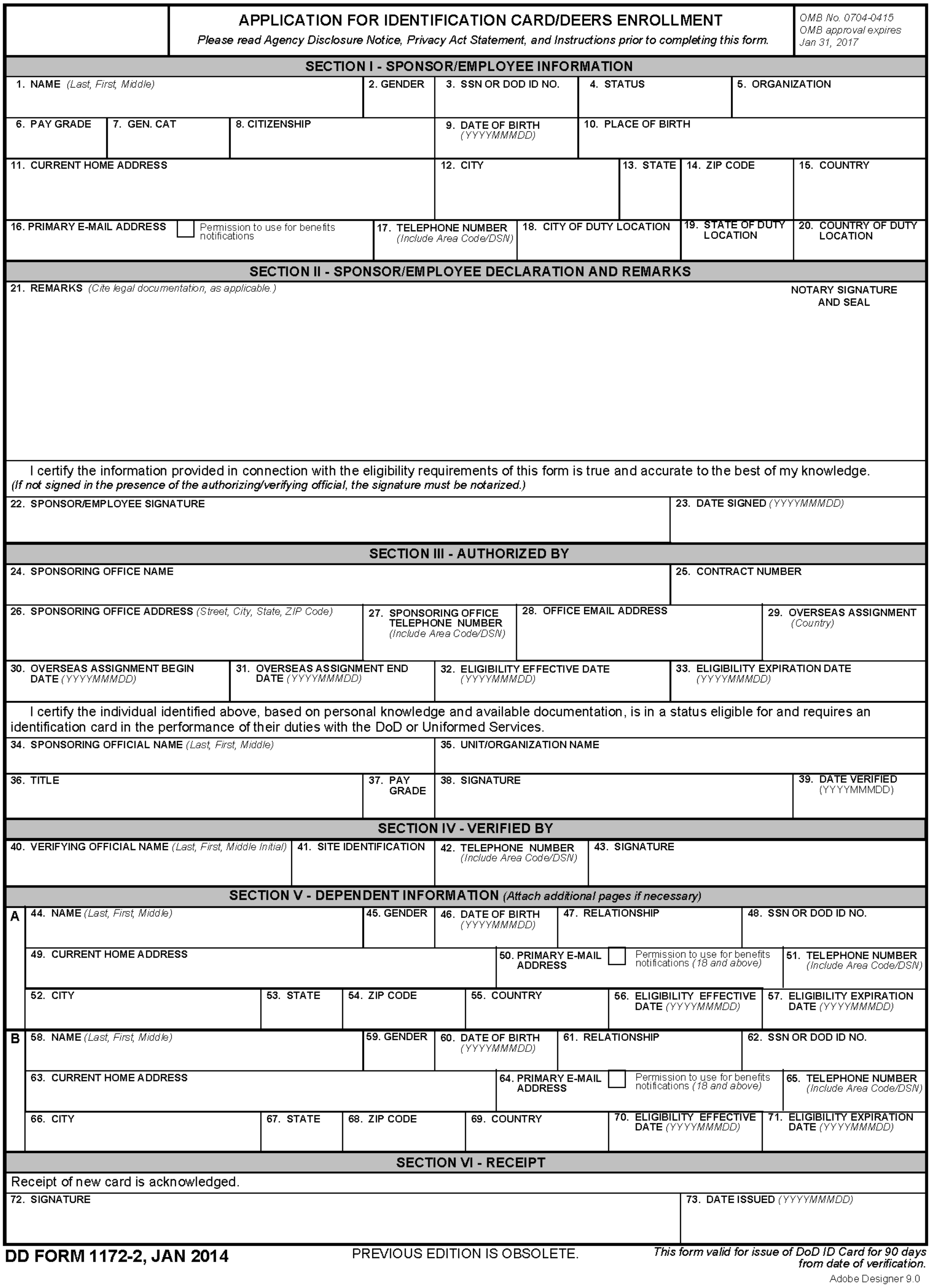
An SPOC can remove TASM/TA accounts in EMMA by completing the following steps:

1. Select the **Site ID** (Organization) for the TASM that requires removal.
2. Select the **TASM role**.
3. In the *Role Details* section, select **Remove User** from the drop-down menu.
4. Select the **Name** of the TASM that requires removal.
5. Click **Go**.
6. In the *Remove User* popup window, click **OK** to confirm removal of the user.
7. Log off when completed.

When removing a TASM/TA account, the SPOC **must**:

- Identify TASMs who require removal
- Assign at least two active TASMs to each Site ID at all times to ensure management of all active TA accounts and associated Applicant records

Appendix A DD Form 1172-2



	APPLICATION FOR IDENTIFICATION CARD/DEERS ENROLLMENT *Please read Agency Disclosure Notice, Privacy Act Statement, and Instructions prior to completing this form.*	*OMB No. 0704-0415* *OMB approval expires* *Jan 31, 2017*

SECTION I - SPONSOR/EMPLOYEE INFORMATION

1. NAME *(Last, First, Middle)*	2. GENDER	3. SSN OR DOD ID NO.	4. STATUS	5. ORGANIZATION
6. PAY GRADE	7. GEN. CAT	8. CITIZENSHIP	9. DATE OF BIRTH *(YYYYMMMDD)*	10. PLACE OF BIRTH

11. CURRENT HOME ADDRESS	12. CITY	13. STATE	14. ZIP CODE	15. COUNTRY
16. PRIMARY E-MAIL ADDRESS □ Permission to use for benefits notifications	17. TELEPHONE NUMBER *(Include Area Code/DSN)*	18. CITY OF DUTY LOCATION	19. STATE OF DUTY LOCATION	20. COUNTRY OF DUTY LOCATION

SECTION II - SPONSOR/EMPLOYEE DECLARATION AND REMARKS

21. REMARKS *(Cite legal documentation, as applicable.)*	NOTARY SIGNATURE AND SEAL

I certify the information provided in connection with the eligibility requirements of this form is true and accurate to the best of my knowledge. ***(If not signed in the presence of the authorizing/verifying official, the signature must be notarized.)***

22. SPONSOR/EMPLOYEE SIGNATURE	23. DATE SIGNED *(YYYYMMMDD)*

SECTION III - AUTHORIZED BY

24. SPONSORING OFFICE NAME	25. CONTRACT NUMBER

26. SPONSORING OFFICE ADDRESS *(Street, City, State, ZIP Code)*	27. SPONSORING OFFICE TELEPHONE NUMBER *(Include Area Code/DSN)*	28. OFFICE EMAIL ADDRESS	29. OVERSEAS ASSIGNMENT *(Country)*
30. OVERSEAS ASSIGNMENT BEGIN DATE *(YYYYMMMDD)*	31. OVERSEAS ASSIGNMENT END DATE *(YYYYMMMDD)*	32. ELIGIBILITY EFFECTIVE DATE *(YYYYMMMDD)*	33. ELIGIBILITY EXPIRATION DATE *(YYYYMMMDD)*

I certify the individual identified above, based on personal knowledge and available documentation, is in a status eligible for and requires an identification card in the performance of their duties with the DoD or Uniformed Services.

34. SPONSORING OFFICIAL NAME *(Last, First, Middle)*	35. UNIT/ORGANIZATION NAME

36. TITLE	37. PAY GRADE	38. SIGNATURE	39. DATE VERIFIED (YYYYMMMDD)

SECTION IV - VERIFIED BY

40. VERIFYING OFFICIAL NAME *(Last, First, Middle Initial)*	41. SITE IDENTIFICATION	42. TELEPHONE NUMBER *(Include Area Code/DSN)*	43. SIGNATURE

SECTION V - DEPENDENT INFORMATION *(Attach additional pages if necessary)*

A

44. NAME *(Last, First, Middle)*	45. GENDER	46. DATE OF BIRTH *(YYYYMMMDD)*	47. RELATIONSHIP	48. SSN OR DOD ID NO.

49. CURRENT HOME ADDRESS	50. PRIMARY E-MAIL ADDRESS □ Permission to use for benefits notifications *(18 and above)*	51. TELEPHONE NUMBER *(Include Area Code/DSN)*

52. CITY	53. STATE	54. ZIP CODE	55. COUNTRY	56. ELIGIBILITY EFFECTIVE DATE *(YYYYMMMDD)*	57. ELIGIBILITY EXPIRATION DATE *(YYYYMMMDD)*

B

58. NAME *(Last, First, Middle)*	59. GENDER	60. DATE OF BIRTH *(YYYYMMMDD)*	61. RELATIONSHIP	62. SSN OR DOD ID NO.

63. CURRENT HOME ADDRESS	64. PRIMARY E-MAIL ADDRESS □ Permission to use for benefits notifications *(18 and above)*	65. TELEPHONE NUMBER *(Include Area Code/DSN)*

66. CITY	67. STATE	68. ZIP CODE	69. COUNTRY	70. ELIGIBILITY EFFECTIVE DATE *(YYYYMMMDD)*	71. ELIGIBILITY EXPIRATION DATE *(YYYYMMMDD)*

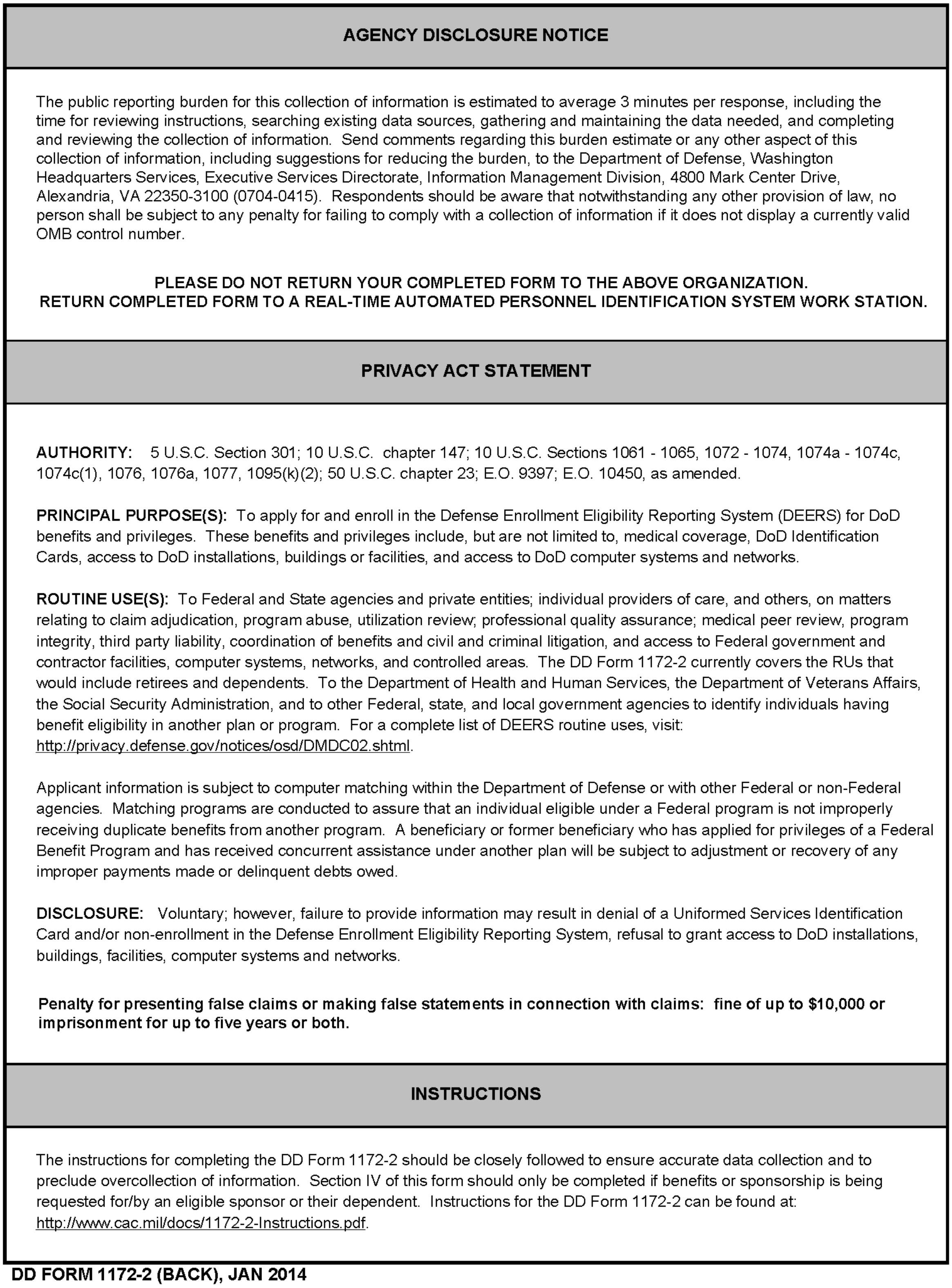
SECTION VI - RECEIPT

Receipt of new card is acknowledged.

72. SIGNATURE	73. DATE ISSUED *(YYYYMMMDD)*

DD FORM 1172-2, JAN 2014 PREVIOUS EDITION IS OBSOLETE. *This form valid for issue of DoD ID Card for 90 days from date of verification.*

Adobe Designer 9.0



AGENCY DISCLOSURE NOTICE

The public reporting burden for this collection of information is estimated to average 3 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to the Department of Defense, Washington Headquarters Services, Executive Services Directorate, Information Management Division, 4800 Mark Center Drive, Alexandria, VA 22350-3100 (0704-0415). Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

**PLEASE DO NOT RETURN YOUR COMPLETED FORM TO THE ABOVE ORGANIZATION.
RETURN COMPLETED FORM TO A REAL-TIME AUTOMATED PERSONNEL IDENTIFICATION SYSTEM WORK STATION.**

PRIVACY ACT STATEMENT

AUTHORITY: 5 U.S.C. Section 301; 10 U.S.C. chapter 147; 10 U.S.C. Sections 1061 - 1065, 1072 - 1074, 1074a - 1074c, 1074c(1), 1076, 1076a, 1077, 1095(k)(2); 50 U.S.C. chapter 23; E.O. 9397; E.O. 10450, as amended.

PRINCIPAL PURPOSE(S): To apply for and enroll in the Defense Enrollment Eligibility Reporting System (DEERS) for DoD benefits and privileges. These benefits and privileges include, but are not limited to, medical coverage, DoD Identification Cards, access to DoD installations, buildings or facilities, and access to DoD computer systems and networks.

ROUTINE USE(S): To Federal and State agencies and private entities; individual providers of care, and others, on matters relating to claim adjudication, program abuse, utilization review; professional quality assurance; medical peer review, program integrity, third party liability, coordination of benefits and civil and criminal litigation, and access to Federal government and contractor facilities, computer systems, networks, and controlled areas. The DD Form 1172-2 currently covers the RUs that would include retirees and dependents. To the Department of Health and Human Services, the Department of Veterans Affairs, the Social Security Administration, and to other Federal, state, and local government agencies to identify individuals having benefit eligibility in another plan or program. For a complete list of DEERS routine uses, visit: http://privacy.defense.gov/notices/osd/DMDC02.shtml.

Applicant information is subject to computer matching within the Department of Defense or with other Federal or non-Federal agencies. Matching programs are conducted to assure that an individual eligible under a Federal program is not improperly receiving duplicate benefits from another program. A beneficiary or former beneficiary who has applied for privileges of a Federal Benefit Program and has received concurrent assistance under another plan will be subject to adjustment or recovery of any improper payments made or delinquent debts owed.

DISCLOSURE: Voluntary; however, failure to provide information may result in denial of a Uniformed Services Identification Card and/or non-enrollment in the Defense Enrollment Eligibility Reporting System, refusal to grant access to DoD installations, buildings, facilities, computer systems and networks.

Penalty for presenting false claims or making false statements in connection with claims: fine of up to $10,000 or imprisonment for up to five years or both.

INSTRUCTIONS

The instructions for completing the DD Form 1172-2 should be closely followed to ensure accurate data collection and to preclude overcollection of information. Section IV of this form should only be completed if benefits or sponsorship is being requested for/by an eligible sponsor or their dependent. Instructions for the DD Form 1172-2 can be found at: http://www.cac.mil/docs/1172-2-Instructions.pdf.

DD FORM 1172-2 (BACK), JAN 2014

Appendix B DD Form 1172-2 Instructions

INSTRUCTIONS FOR COMPLETION OF DD FORM 1172-2, "APPLICATION FOR IDENTIFICATION CARD/DEERS ENROLLMENT"

The DD Form 1172-2 shall be used to apply for issuance of a DD Form 2 (Reserve, Retired, and Reserve Retired), a DD Form 1173, a DD Form 1173-1, a DD Form 2764, a DD Form 2765, and a Common Access Card (CAC) for eligible individuals who are not enrolled in the Defense Enrollment Eligibility Reporting System (DEERS). The DD Form 1172-2 shall also be used to enroll eligible individuals in DEERS or to update an eligible individual's DEERS record by submitting the form to a Verifying Official (VO) at any Real-time Automated Personnel Identification System (RAPIDS) Site. Retention and disposition of the DD Form 1172-2 shall be in accordance with uniformed services' regulatory instructions.

Notes:

- DoD sponsors enrolling their dependents in DEERS should complete Sections I, II, and V.
    - For dependents already enrolled in DEERS, CAC-enabled sponsors may logon to the RAPIDS Self-Service (RSS) Portal to verify their dependents online and digitally create and sign DD Form 1172-2. Once the CAC-enabled sponsor verifies the dependent via RSS portal, the DD Form 1172-2 is saved under the dependent's DEERS record, and must be printed and submitted to a VO at a RAPIDS Site to support card issuance.

- DoD sponsors updating their own status or adding a personnel condition impacting benefits (e.g., overseas assignment) should complete Sections I and II.

- Eligible employees applying for a CAC should complete Sections I and II (and Section IV if a Foreign Affiliate on orders to the U.S. with authorized dependents). The DD Form 1172-2 should then be provided to a DoD sponsor for authorization and completion of Section III.

- DoD personnel sponsoring an eligible individual for a CAC should complete Section III.

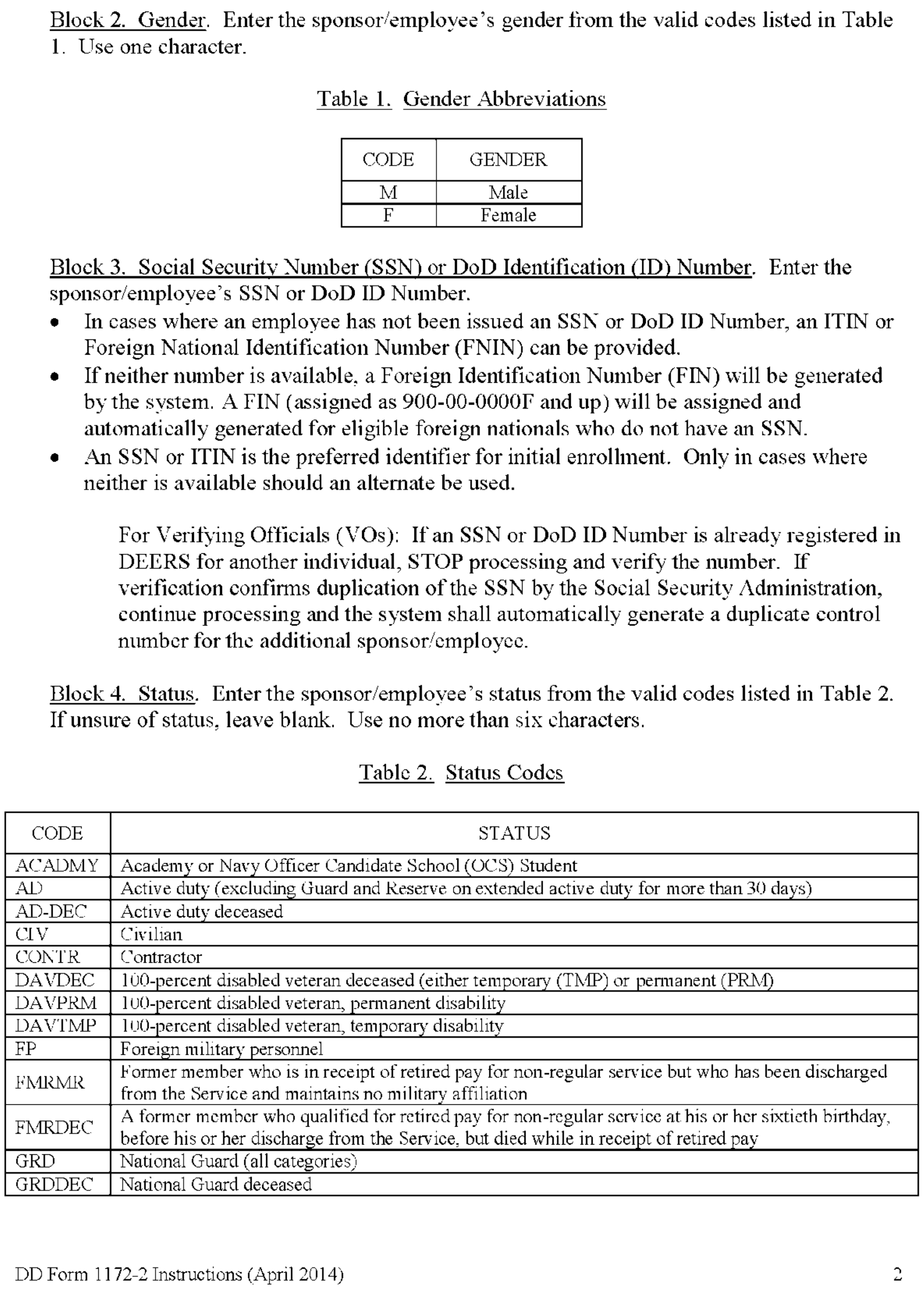
- For certain populations, a paper form will not be required (e.g., populations entered into RAPIDS via the Trusted Associate Sponsorship System (TASS)).

- A DD Form 577 (signature card) for DoD personnel completing Section III must be on file at the issuing site for CAC applicants using the DD Form 1172-2 for enrollment. The DD Form 577 may be completed with either a wet or digital signature, selecting the format which will be used to sign the DD Form 1172-2. If both signature formats will be used, a DD Form 577 for each format must be completed and on file at the issuing site.

SECTION I – SPONSOR/EMPLOYEE INFORMATION

Block 1. Name. Enter the sponsor/employee's LAST name first, enter the FIRST name, and then enter the MIDDLE initial or the full MIDDLE name. Use no more than 51 characters.

- The name field can include a designation of JR, SR, ESQ, or the Roman numerals I through X. To include that designation, enter the appropriate data after the middle initial.
- The name cannot contain any special characters nor is any punctuation permitted.



Block 2. Gender. Enter the sponsor/employee's gender from the valid codes listed in Table 1. Use one character.

Table 1. Gender Abbreviations

CODE	GENDER
M	Male
F	Female

Block 3. Social Security Number (SSN) or DoD Identification (ID) Number. Enter the sponsor/employee's SSN or DoD ID Number.

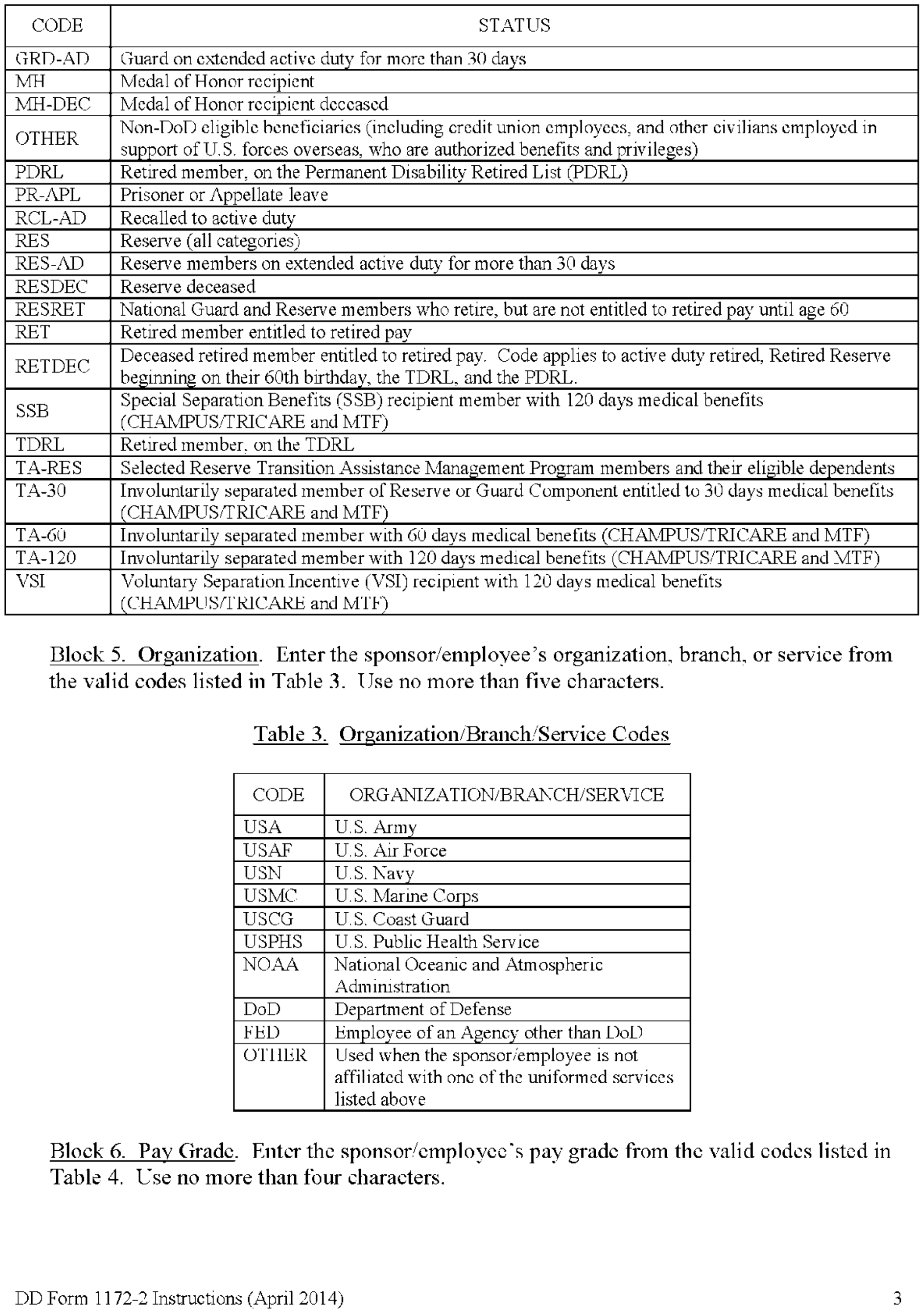
- In cases where an employee has not been issued an SSN or DoD ID Number, an ITIN or Foreign National Identification Number (FNIN) can be provided.
- If neither number is available, a Foreign Identification Number (FIN) will be generated by the system. A FIN (assigned as 900-00-0000F and up) will be assigned and automatically generated for eligible foreign nationals who do not have an SSN.
- An SSN or ITIN is the preferred identifier for initial enrollment. Only in cases where neither is available should an alternate be used.

> For Verifying Officials (VOs): If an SSN or DoD ID Number is already registered in DEERS for another individual, STOP processing and verify the number. If verification confirms duplication of the SSN by the Social Security Administration, continue processing and the system shall automatically generate a duplicate control number for the additional sponsor/employee.

Block 4. Status. Enter the sponsor/employee's status from the valid codes listed in Table 2. If unsure of status, leave blank. Use no more than six characters.

Table 2. Status Codes

CODE	STATUS
ACADMY	Academy or Navy Officer Candidate School (OCS) Student
AD	Active duty (excluding Guard and Reserve on extended active duty for more than 30 days)
AD-DEC	Active duty deceased
CIV	Civilian
CONTR	Contractor
DAVDEC	100-percent disabled veteran deceased (either temporary (TMP) or permanent (PRM)
DAVPRM	100-percent disabled veteran, permanent disability
DAVTMP	100-percent disabled veteran, temporary disability
FP	Foreign military personnel
FMRMR	Former member who is in receipt of retired pay for non-regular service but who has been discharged from the Service and maintains no military affiliation
FMRDEC	A former member who qualified for retired pay for non-regular service at his or her sixtieth birthday, before his or her discharge from the Service, but died while in receipt of retired pay
GRD	National Guard (all categories)
GRDDEC	National Guard deceased



CODE	STATUS
GRD-AD	Guard on extended active duty for more than 30 days
MH	Medal of Honor recipient
MH-DEC	Medal of Honor recipient deceased
OTHER	Non-DoD eligible beneficiaries (including credit union employees, and other civilians employed in support of U.S. forces overseas, who are authorized benefits and privileges)
PDRL	Retired member, on the Permanent Disability Retired List (PDRL)
PR-APL	Prisoner or Appellate leave
RCL-AD	Recalled to active duty
RES	Reserve (all categories)
RES-AD	Reserve members on extended active duty for more than 30 days
RESDEC	Reserve deceased
RESRET	National Guard and Reserve members who retire, but are not entitled to retired pay until age 60
RET	Retired member entitled to retired pay
RETDEC	Deceased retired member entitled to retired pay. Code applies to active duty retired, Retired Reserve beginning on their 60th birthday, the TDRL, and the PDRL.
SSB	Special Separation Benefits (SSB) recipient member with 120 days medical benefits (CHAMPUS/TRICARE and MTF)
TDRL	Retired member, on the TDRL
TA-RES	Selected Reserve Transition Assistance Management Program members and their eligible dependents
TA-30	Involuntarily separated member of Reserve or Guard Component entitled to 30 days medical benefits (CHAMPUS/TRICARE and MTF)
TA-60	Involuntarily separated member with 60 days medical benefits (CHAMPUS/TRICARE and MTF)
TA-120	Involuntarily separated member with 120 days medical benefits (CHAMPUS/TRICARE and MTF)
VSI	Voluntary Separation Incentive (VSI) recipient with 120 days medical benefits (CHAMPUS/TRICARE and MTF)

Block 5. Organization. Enter the sponsor/employee's organization, branch, or service from the valid codes listed in Table 3. Use no more than five characters.

Table 3. Organization/Branch/Service Codes

CODE	ORGANIZATION/BRANCH/SERVICE
USA	U.S. Army
USAF	U.S. Air Force
USN	U.S. Navy
USMC	U.S. Marine Corps
USCG	U.S. Coast Guard
USPHS	U.S. Public Health Service
NOAA	National Oceanic and Atmospheric Administration
DoD	Department of Defense
FED	Employee of an Agency other than DoD
OTHER	Used when the sponsor/employee is not affiliated with one of the uniformed services listed above

Block 6. Pay Grade. Enter the sponsor/employee's pay grade from the valid codes listed in Table 4. Use no more than four characters.

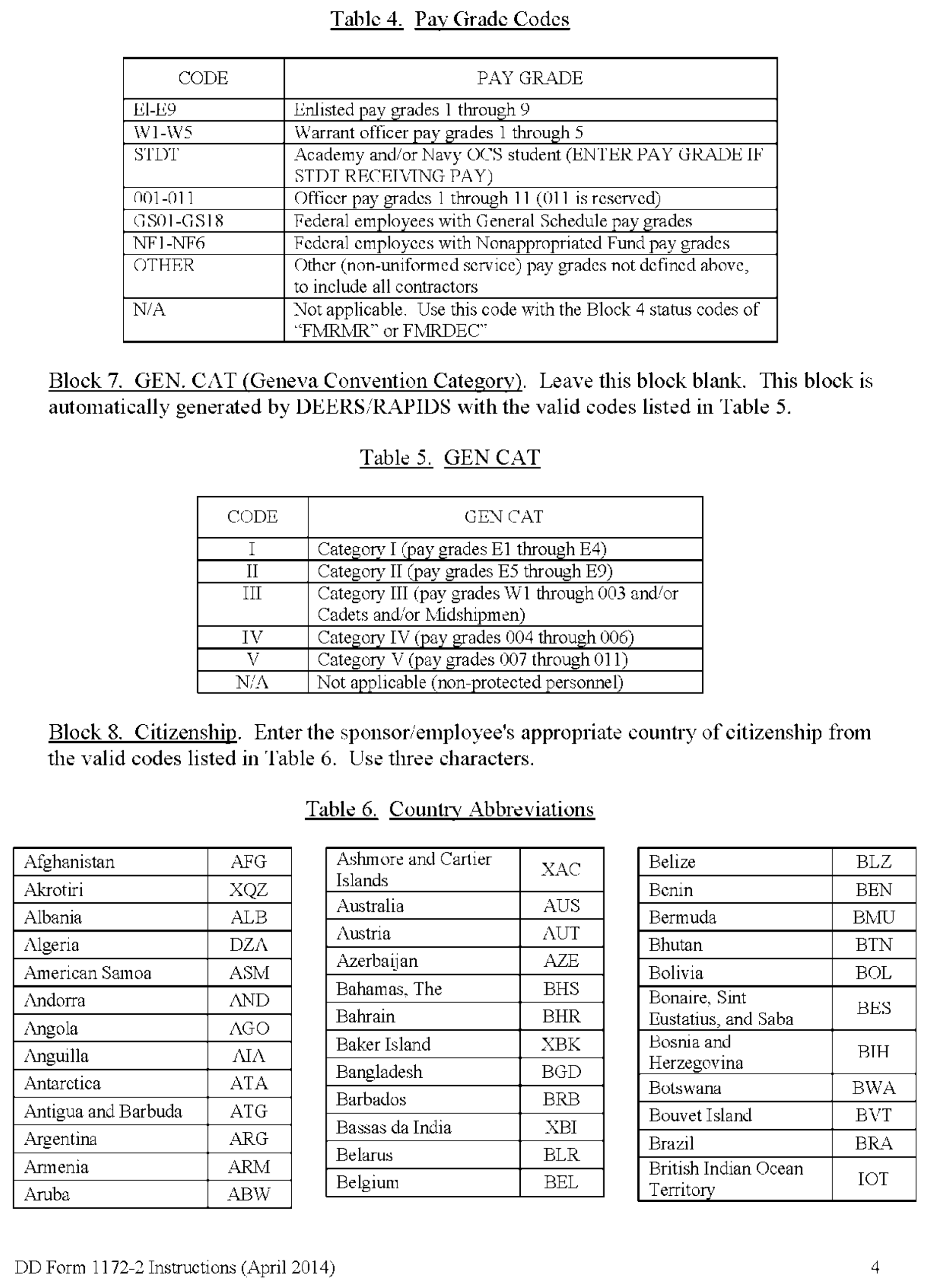


Table 4. Pay Grade Codes

CODE	PAY GRADE
EI-E9	Enlisted pay grades 1 through 9
W1-W5	Warrant officer pay grades 1 through 5
STDT	Academy and/or Navy OCS student (ENTER PAY GRADE IF STDT RECEIVING PAY)
001-011	Officer pay grades 1 through 11 (011 is reserved)
GS01-GS18	Federal employees with General Schedule pay grades
NF1-NF6	Federal employees with Nonappropriated Fund pay grades
OTHER	Other (non-uniformed service) pay grades not defined above, to include all contractors
N/A	Not applicable. Use this code with the Block 4 status codes of “FMRMR” or FMRDEC”

Block 7. GEN. CAT (Geneva Convention Category). Leave this block blank. This block is automatically generated by DEERS/RAPIDS with the valid codes listed in Table 5.

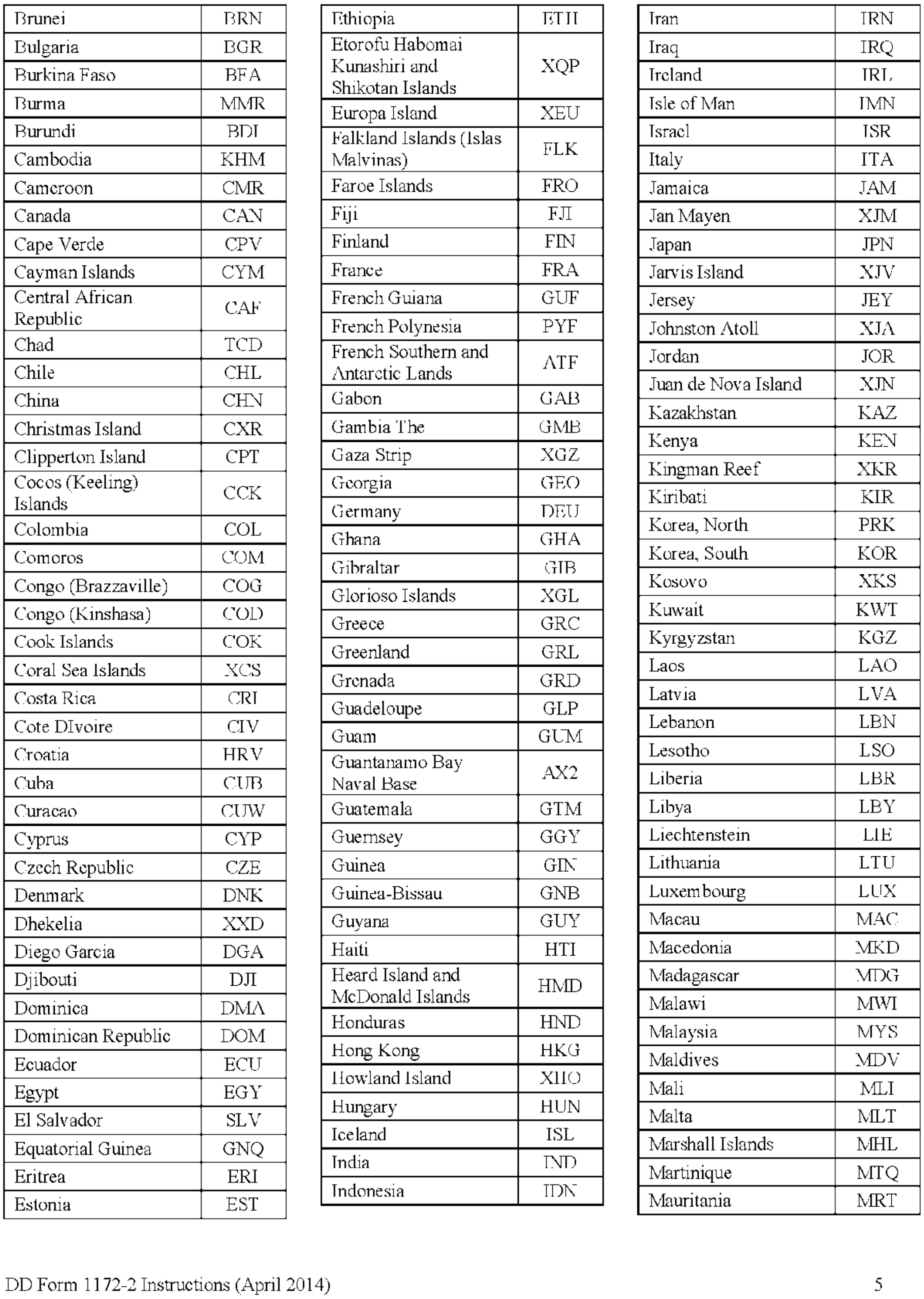
Table 5. GEN CAT

CODE	GEN CAT
I	Category I (pay grades E1 through E4)
II	Category II (pay grades E5 through E9)
III	Category III (pay grades W1 through 003 and/or Cadets and/or Midshipmen)
IV	Category IV (pay grades 004 through 006)
V	Category V (pay grades 007 through 011)
N/A	Not applicable (non-protected personnel)

Block 8. Citizenship. Enter the sponsor/employee's appropriate country of citizenship from the valid codes listed in Table 6. Use three characters.

Table 6. Country Abbreviations

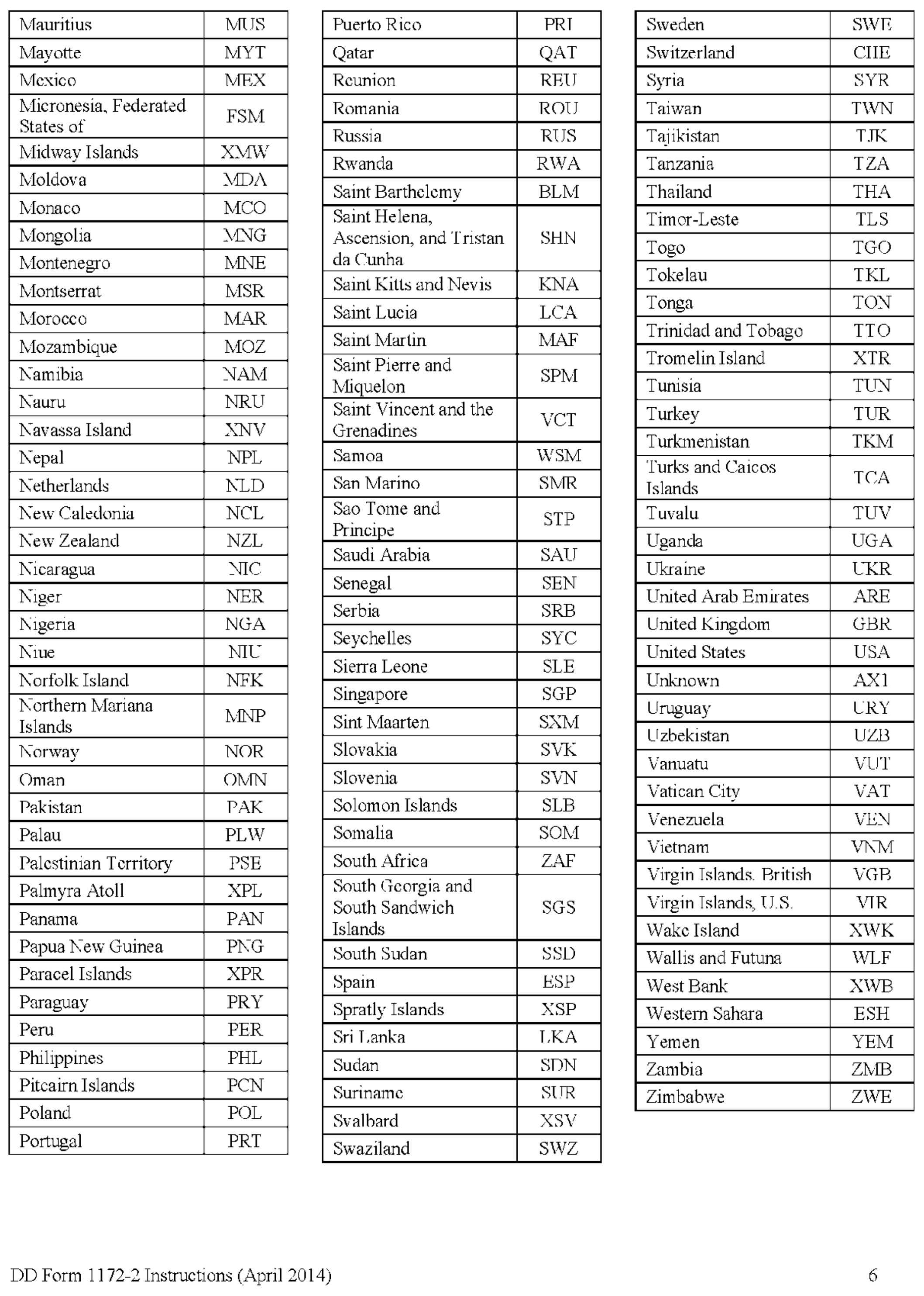
Afghanistan	AFG
Akrotiri	XQZ
Albania	ALB
Algeria	DZA
American Samoa	ASM
Andorra	AND
Angola	AGO
Anguilla	AIA
Antarctica	ATA
Antigua and Barbuda	ATG
Argentina	ARG
Armenia	ARM
Aruba	ABW
Ashmore and Cartier Islands	XAC
Australia	AUS
Austria	AUT
Azerbaijan	AZE
Bahamas, The	BHS
Bahrain	BHR
Baker Island	XBK
Bangladesh	BGD
Barbados	BRB
Bassas da India	XBI
Belarus	BLR
Belgium	BEL
Belize	BLZ
Benin	BEN
Bermuda	BMU
Bhutan	BTN
Bolivia	BOL
Bonaire, Sint Eustatius, and Saba	BES
Bosnia and Herzegovina	BIH
Botswana	BWA
Bouvet Island	BVT
Brazil	BRA
British Indian Ocean Territory	IOT



Brunei	BRN
Bulgaria	BGR
Burkina Faso	BFA
Burma	MMR
Burundi	BDI
Cambodia	KHM
Cameroon	CMR
Canada	CAN
Cape Verde	CPV
Cayman Islands	CYM
Central African Republic	CAF
Chad	TCD
Chile	CHL
China	CHN
Christmas Island	CXR
Clipperton Island	CPT
Cocos (Keeling) Islands	CCK
Colombia	COL
Comoros	COM
Congo (Brazzaville)	COG
Congo (Kinshasa)	COD
Cook Islands	COK
Coral Sea Islands	XCS
Costa Rica	CRI
Cote DIvoire	CIV
Croatia	HRV
Cuba	CUB
Curacao	CUW
Cyprus	CYP
Czech Republic	CZE
Denmark	DNK
Dhekelia	XXD
Diego Garcia	DGA
Djibouti	DJI
Dominica	DMA
Dominican Republic	DOM
Ecuador	ECU
Egypt	EGY
El Salvador	SLV
Equatorial Guinea	GNQ
Eritrea	ERI
Estonia	EST

Ethiopia	ETH
Etorofu Habomai Kunashiri and Shikotan Islands	XQP
Europa Island	XEU
Falkland Islands (Islas Malvinas)	FLK
Faroe Islands	FRO
Fiji	FJI
Finland	FIN
France	FRA
French Guiana	GUF
French Polynesia	PYF
French Southern and Antarctic Lands	ATF
Gabon	GAB
Gambia The	GMB
Gaza Strip	XGZ
Georgia	GEO
Germany	DEU
Ghana	GHA
Gibraltar	GIB
Glorioso Islands	XGL
Greece	GRC
Greenland	GRL
Grenada	GRD
Guadeloupe	GLP
Guam	GUM
Guantanamo Bay Naval Base	AX2
Guatemala	GTM
Guernsey	GGY
Guinea	GIN
Guinea-Bissau	GNB
Guyana	GUY
Haiti	HTI
Heard Island and McDonald Islands	HMD
Honduras	HND
Hong Kong	HKG
Howland Island	XHO
Hungary	HUN
Iceland	ISL
India	IND
Indonesia	IDN

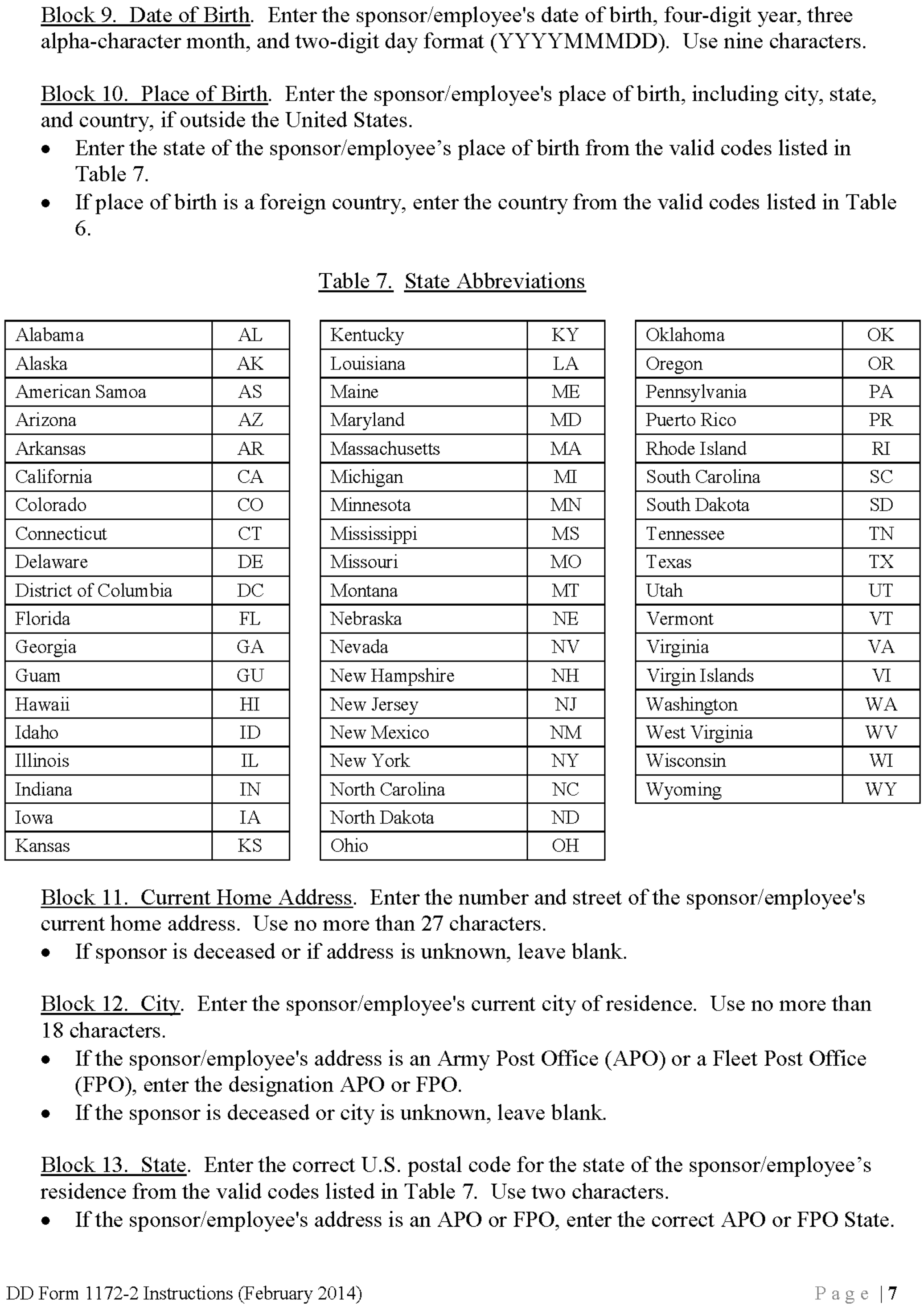
Iran	IRN
Iraq	IRQ
Ireland	IRL
Isle of Man	IMN
Israel	ISR
Italy	ITA
Jamaica	JAM
Jan Mayen	XJM
Japan	JPN
Jarvis Island	XJV
Jersey	JEY
Johnston Atoll	XJA
Jordan	JOR
Juan de Nova Island	XJN
Kazakhstan	KAZ
Kenya	KEN
Kingman Reef	XKR
Kiribati	KIR
Korea, North	PRK
Korea, South	KOR
Kosovo	XKS
Kuwait	KWT
Kyrgyzstan	KGZ
Laos	LAO
Latvia	LVA
Lebanon	LBN
Lesotho	LSO
Liberia	LBR
Libya	LBY
Liechtenstein	LIE
Lithuania	LTU
Luxembourg	LUX
Macau	MAC
Macedonia	MKD
Madagascar	MDG
Malawi	MWI
Malaysia	MYS
Maldives	MDV
Mali	MLI
Malta	MLT
Marshall Islands	MHL
Martinique	MTQ
Mauritania	MRT



Mauritius	MUS
Mayotte	MYT
Mexico	MEX
Micronesia, Federated States of	FSM
Midway Islands	XMW
Moldova	MDA
Monaco	MCO
Mongolia	MNG
Montenegro	MNE
Montserrat	MSR
Morocco	MAR
Mozambique	MOZ
Namibia	NAM
Nauru	NRU
Navassa Island	XNV
Nepal	NPL
Netherlands	NLD
New Caledonia	NCL
New Zealand	NZL
Nicaragua	NIC
Niger	NER
Nigeria	NGA
Niue	NIU
Norfolk Island	NFK
Northern Mariana Islands	MNP
Norway	NOR
Oman	OMN
Pakistan	PAK
Palau	PLW
Palestinian Territory	PSE
Palmyra Atoll	XPL
Panama	PAN
Papua New Guinea	PNG
Paracel Islands	XPR
Paraguay	PRY
Peru	PER
Philippines	PHL
Pitcairn Islands	PCN
Poland	POL
Portugal	PRT

Puerto Rico	PRI
Qatar	QAT
Reunion	REU
Romania	ROU
Russia	RUS
Rwanda	RWA
Saint Barthelemy	BLM
Saint Helena, Ascension, and Tristan da Cunha	SHN
Saint Kitts and Nevis	KNA
Saint Lucia	LCA
Saint Martin	MAF
Saint Pierre and Miquelon	SPM
Saint Vincent and the Grenadines	VCT
Samoa	WSM
San Marino	SMR
Sao Tome and Principe	STP
Saudi Arabia	SAU
Senegal	SEN
Serbia	SRB
Seychelles	SYC
Sierra Leone	SLE
Singapore	SGP
Sint Maarten	SXM
Slovakia	SVK
Slovenia	SVN
Solomon Islands	SLB
Somalia	SOM
South Africa	ZAF
South Georgia and South Sandwich Islands	SGS
South Sudan	SSD
Spain	ESP
Spratly Islands	XSP
Sri Lanka	LKA
Sudan	SDN
Suriname	SUR
Svalbard	XSV
Swaziland	SWZ

Sweden	SWE
Switzerland	CHE
Syria	SYR
Taiwan	TWN
Tajikistan	TJK
Tanzania	TZA
Thailand	THA
Timor-Leste	TLS
Togo	TGO
Tokelau	TKL
Tonga	TON
Trinidad and Tobago	TTO
Tromelin Island	XTR
Tunisia	TUN
Turkey	TUR
Turkmenistan	TKM
Turks and Caicos Islands	TCA
Tuvalu	TUV
Uganda	UGA
Ukraine	UKR
United Arab Emirates	ARE
United Kingdom	GBR
United States	USA
Unknown	AX1
Uruguay	URY
Uzbekistan	UZB
Vanuatu	VUT
Vatican City	VAT
Venezuela	VEN
Vietnam	VNM
Virgin Islands, British	VGB
Virgin Islands, U.S.	VIR
Wake Island	XWK
Wallis and Futuna	WLF
West Bank	XWB
Western Sahara	ESH
Yemen	YEM
Zambia	ZMB
Zimbabwe	ZWE



Block 9. Date of Birth. Enter the sponsor/employee's date of birth, four-digit year, three alpha-character month, and two-digit day format (YYYYMMMDD). Use nine characters.

Block 10. Place of Birth. Enter the sponsor/employee's place of birth, including city, state, and country, if outside the United States.

- Enter the state of the sponsor/employee's place of birth from the valid codes listed in Table 7.
- If place of birth is a foreign country, enter the country from the valid codes listed in Table 6.

Table 7. State Abbreviations

Alabama	AL	Kentucky	KY	Oklahoma	OK
Alaska	AK	Louisiana	LA	Oregon	OR
American Samoa	AS	Maine	ME	Pennsylvania	PA
Arizona	AZ	Maryland	MD	Puerto Rico	PR
Arkansas	AR	Massachusetts	MA	Rhode Island	RI
California	CA	Michigan	MI	South Carolina	SC
Colorado	CO	Minnesota	MN	South Dakota	SD
Connecticut	CT	Mississippi	MS	Tennessee	TN
Delaware	DE	Missouri	MO	Texas	TX
District of Columbia	DC	Montana	MT	Utah	UT
Florida	FL	Nebraska	NE	Vermont	VT
Georgia	GA	Nevada	NV	Virginia	VA
Guam	GU	New Hampshire	NH	Virgin Islands	VI
Hawaii	HI	New Jersey	NJ	Washington	WA
Idaho	ID	New Mexico	NM	West Virginia	WV
Illinois	IL	New York	NY	Wisconsin	WI
Indiana	IN	North Carolina	NC	Wyoming	WY
Iowa	IA	North Dakota	ND		
Kansas	KS	Ohio	OH		

Block 11. Current Home Address. Enter the number and street of the sponsor/employee's current home address. Use no more than 27 characters.

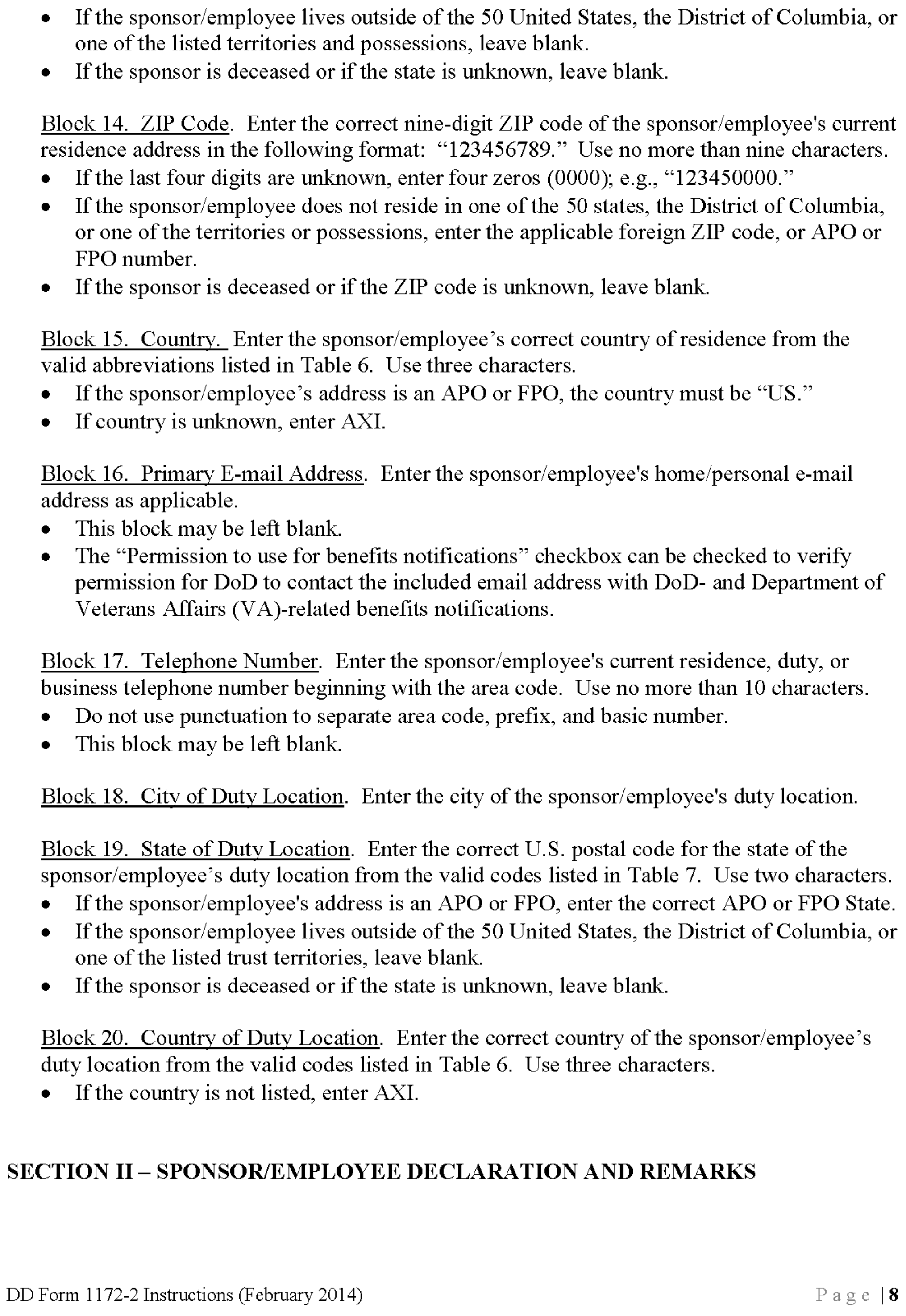
- If sponsor is deceased or if address is unknown, leave blank.

Block 12. City. Enter the sponsor/employee's current city of residence. Use no more than 18 characters.

- If the sponsor/employee's address is an Army Post Office (APO) or a Fleet Post Office (FPO), enter the designation APO or FPO.
- If the sponsor is deceased or city is unknown, leave blank.

Block 13. State. Enter the correct U.S. postal code for the state of the sponsor/employee's residence from the valid codes listed in Table 7. Use two characters.

- If the sponsor/employee's address is an APO or FPO, enter the correct APO or FPO State.



- If the sponsor/employee lives outside of the 50 United States, the District of Columbia, or one of the listed territories and possessions, leave blank.
- If the sponsor is deceased or if the state is unknown, leave blank.

Block 14. ZIP Code. Enter the correct nine-digit ZIP code of the sponsor/employee's current residence address in the following format: "123456789." Use no more than nine characters.

- If the last four digits are unknown, enter four zeros (0000); e.g., "123450000."
- If the sponsor/employee does not reside in one of the 50 states, the District of Columbia, or one of the territories or possessions, enter the applicable foreign ZIP code, or APO or FPO number.
- If the sponsor is deceased or if the ZIP code is unknown, leave blank.

Block 15. Country. Enter the sponsor/employee's correct country of residence from the valid abbreviations listed in Table 6. Use three characters.

- If the sponsor/employee's address is an APO or FPO, the country must be "US."
- If country is unknown, enter AXI.

Block 16. Primary E-mail Address. Enter the sponsor/employee's home/personal e-mail address as applicable.

- This block may be left blank.
- The "Permission to use for benefits notifications" checkbox can be checked to verify permission for DoD to contact the included email address with DoD- and Department of Veterans Affairs (VA)-related benefits notifications.

Block 17. Telephone Number. Enter the sponsor/employee's current residence, duty, or business telephone number beginning with the area code. Use no more than 10 characters.

- Do not use punctuation to separate area code, prefix, and basic number.
- This block may be left blank.

Block 18. City of Duty Location. Enter the city of the sponsor/employee's duty location.

Block 19. State of Duty Location. Enter the correct U.S. postal code for the state of the sponsor/employee's duty location from the valid codes listed in Table 7. Use two characters.

- If the sponsor/employee's address is an APO or FPO, enter the correct APO or FPO State.
- If the sponsor/employee lives outside of the 50 United States, the District of Columbia, or one of the listed trust territories, leave blank.
- If the sponsor is deceased or if the state is unknown, leave blank.

Block 20. Country of Duty Location. Enter the correct country of the sponsor/employee's duty location from the valid codes listed in Table 6. Use three characters.

- If the country is not listed, enter AXI.

SECTION II – SPONSOR/EMPLOYEE DECLARATION AND REMARKS

Block 21. Remarks. Enter the method of verification and further explanation of qualifying status.

- Qualifying status may include SF 52, sponsoring agency, and period of DEERS enrollment, or other appropriate comments, such as particular work assignment.
- This section may be left blank, or prepopulated by the VO.

Block 22. Sponsor/Employee Signature. Block must contain the sponsor/employee's signature.

- When the DD Form 1172-2 is not signed in the presence of the VO at the time of DEERS enrollment, the signature must be notarized. The notary seal and signature should be placed in the right margin of Block 21.
- The following exceptions to this requirement are authorized:
  1. Unremarried or unmarried former spouses shall sign for themselves.
  2. When the sponsor is deceased, the survivors shall sign for themselves.
  3. When the sponsor is unavailable for signature, the VO shall ensure that the dependency between the sponsor and family member exists. The VO shall follow the guidance provided in the applicable Uniformed Service regulation.

Block 23. Date Signed. Enter the date, four-digit year, three alpha-character month, and two-digit day format (YYYYMMMDD), that the DD Form 1172-2 Block 22 was signed.

SECTION III – AUTHORIZED BY (DoD CAC Sponsors Only)

Block 24. Sponsoring Office Name. Enter the name of the organization the employee works for or is assigned to.

- The sponsoring official shall be a uniformed service member or civilian employee working for the sponsoring organization.

Block 25. Contract Number. Enter the contract number for the purposes of entry into the TASS.

Block 26. Sponsoring Office Address. Enter the number and street, city, state, and zip code of the employee's sponsoring office address. See Table 7 for state abbreviations.

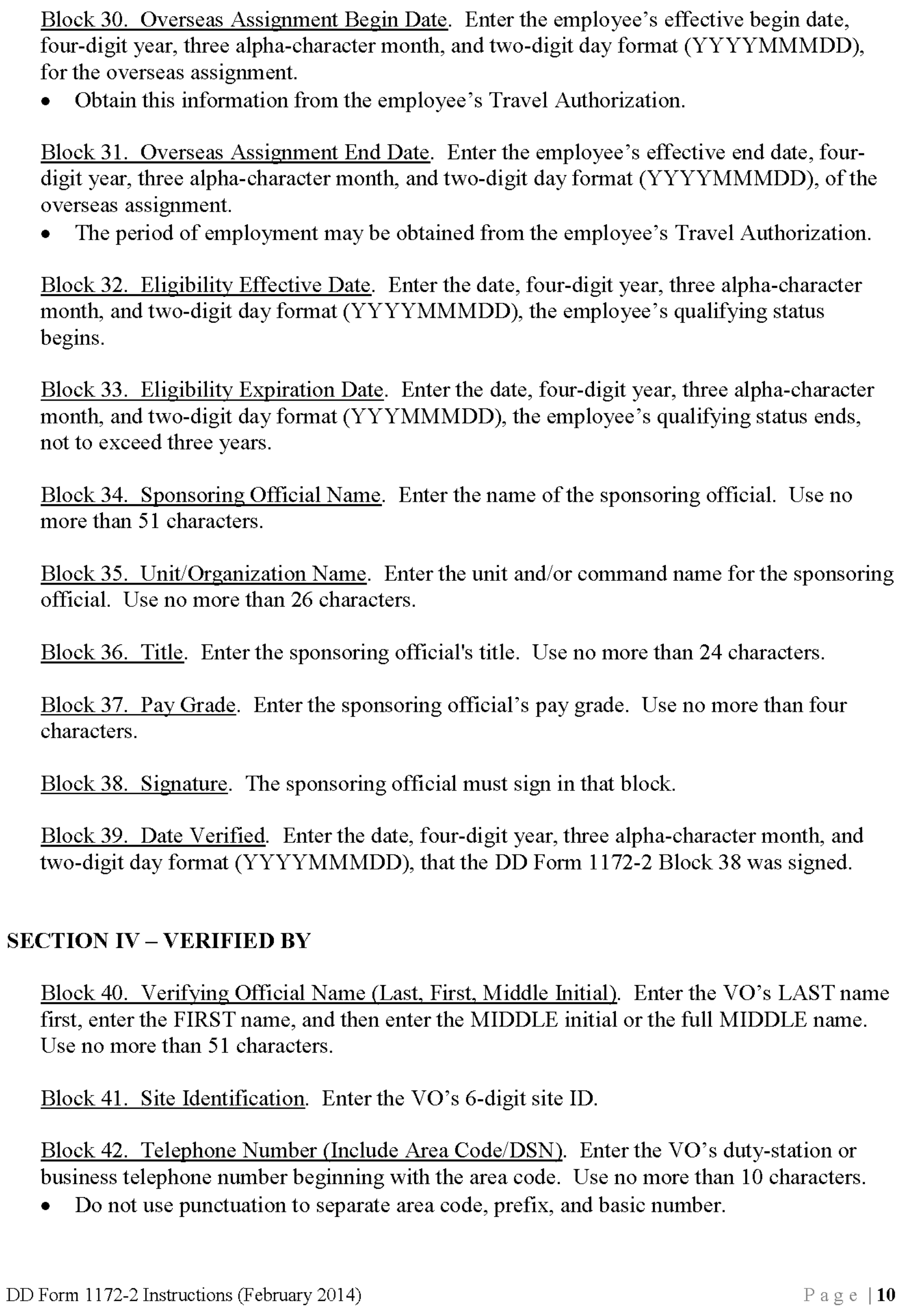
Block 27. Sponsoring Office Telephone Number. Enter the sponsoring office telephone number beginning with the area code. Use no more than 14 characters.

- Do not use punctuation to separate area code, prefix, and basic number.

Block 28. Office Email Address. Enter the employee's office e-mail address, as applicable.

Block 29. Overseas Assignment. Enter the employee's country of assignment. See Table 6 for country codes.

- Obtain this information from the employee's Travel Authorization.



Block 30. Overseas Assignment Begin Date. Enter the employee's effective begin date, four-digit year, three alpha-character month, and two-digit day format (YYYYMMMDD), for the overseas assignment.

- Obtain this information from the employee's Travel Authorization.

Block 31. Overseas Assignment End Date. Enter the employee's effective end date, four-digit year, three alpha-character month, and two-digit day format (YYYYMMMDD), of the overseas assignment.

- The period of employment may be obtained from the employee's Travel Authorization.

Block 32. Eligibility Effective Date. Enter the date, four-digit year, three alpha-character month, and two-digit day format (YYYYMMMDD), the employee's qualifying status begins.

Block 33. Eligibility Expiration Date. Enter the date, four-digit year, three alpha-character month, and two-digit day format (YYYMMMDD), the employee's qualifying status ends, not to exceed three years.

Block 34. Sponsoring Official Name. Enter the name of the sponsoring official. Use no more than 51 characters.

Block 35. Unit/Organization Name. Enter the unit and/or command name for the sponsoring official. Use no more than 26 characters.

Block 36. Title. Enter the sponsoring official's title. Use no more than 24 characters.

Block 37. Pay Grade. Enter the sponsoring official's pay grade. Use no more than four characters.

Block 38. Signature. The sponsoring official must sign in that block.

Block 39. Date Verified. Enter the date, four-digit year, three alpha-character month, and two-digit day format (YYYYMMMDD), that the DD Form 1172-2 Block 38 was signed.

SECTION IV – VERIFIED BY

Block 40. Verifying Official Name (Last, First, Middle Initial). Enter the VO's LAST name first, enter the FIRST name, and then enter the MIDDLE initial or the full MIDDLE name. Use no more than 51 characters.

Block 41. Site Identification. Enter the VO's 6-digit site ID.

Block 42. Telephone Number (Include Area Code/DSN). Enter the VO's duty-station or business telephone number beginning with the area code. Use no more than 10 characters.

- Do not use punctuation to separate area code, prefix, and basic number.

Block 43. Signature. VO must sign in the block.

SECTION V – DEPENDENT INFORMATION

Section A (Blocks 40-51)

Block 44. Name. Enter the dependent's LAST name first, enter the FIRST name, and then enter the MIDDLE initial or the full MIDDLE name. Use no more than 51 characters.

- The name field can include a designation of JR, SR, ESQ, or the Roman numerals I through X. To include that designation, enter the appropriate data after the middle initial.
- The name cannot contain any special characters nor is any punctuation permitted.

Block 45. Gender. Enter the dependent's gender from the valid codes listed in Table 1. Use one character.

Block 46. Date of Birth. Enter the dependent's date of birth, four-digit year, three alpha character month, and two-digit day format (YYYYMMMDD).

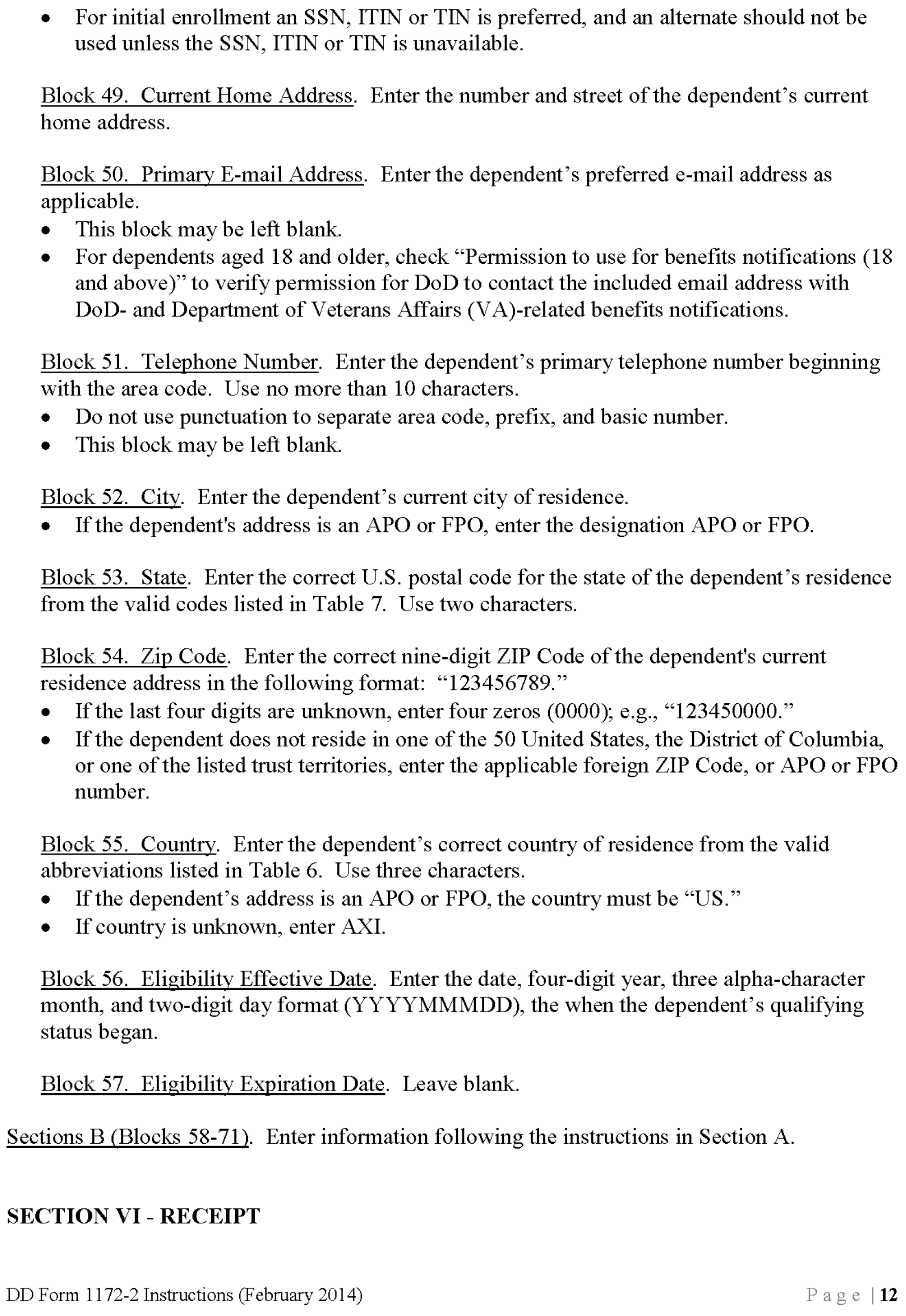
Block 47. Relationship. Enter the dependent's relationship to the sponsor from the valid abbreviations listed in Table 9.

Table 9. Relationship Codes

CODE	RELATIONSHIP
CH	Child
DB	DoD Beneficiary
FC	Foster Child
PAR	Parent
PL	Parent-in-law
PACH	Pre-adoptive Child
SP	Spouse
SC	Stepchild
STP	Stepparent
SPL	Stepparent-in-law
UMW	Unmarried Widow(er)
URW	Unremarried Widow(er)
WARD	Ward

Block 48. SSN or DoD ID Number. Enter the dependent's SSN, DoD ID number, ITIN or temporary identification number (TIN).

- A TIN will be automatically generated by RAPIDS and assigned for categories of beneficiaries who do not yet have SSNs, such as newborns and foreign spouses, awaiting an SSN, or for those who do not have and are not eligible for an SSN. Direct care at military treatment facilities will be suspended if an SSN is not provided within 270 days.



- For initial enrollment an SSN, ITIN or TIN is preferred, and an alternate should not be used unless the SSN, ITIN or TIN is unavailable.

Block 49. Current Home Address. Enter the number and street of the dependent’s current home address.

Block 50. Primary E-mail Address. Enter the dependent’s preferred e-mail address as applicable.

- This block may be left blank.
- For dependents aged 18 and older, check “Permission to use for benefits notifications (18 and above)” to verify permission for DoD to contact the included email address with DoD- and Department of Veterans Affairs (VA)-related benefits notifications.

Block 51. Telephone Number. Enter the dependent’s primary telephone number beginning with the area code. Use no more than 10 characters.

- Do not use punctuation to separate area code, prefix, and basic number.
- This block may be left blank.

Block 52. City. Enter the dependent’s current city of residence.

- If the dependent's address is an APO or FPO, enter the designation APO or FPO.

Block 53. State. Enter the correct U.S. postal code for the state of the dependent’s residence from the valid codes listed in Table 7. Use two characters.

Block 54. Zip Code. Enter the correct nine-digit ZIP Code of the dependent's current residence address in the following format: “123456789.”

- If the last four digits are unknown, enter four zeros (0000); e.g., “123450000.”
- If the dependent does not reside in one of the 50 United States, the District of Columbia, or one of the listed trust territories, enter the applicable foreign ZIP Code, or APO or FPO number.

Block 55. Country. Enter the dependent’s correct country of residence from the valid abbreviations listed in Table 6. Use three characters.

- If the dependent’s address is an APO or FPO, the country must be “US.”
- If country is unknown, enter AXI.

Block 56. Eligibility Effective Date. Enter the date, four-digit year, three alpha-character month, and two-digit day format (YYYYMMMDD), the when the dependent’s qualifying status began.

Block 57. Eligibility Expiration Date. Leave blank.

Sections B (Blocks 58-71). Enter information following the instructions in Section A.

SECTION VI - RECEIPT

Block 72. Signature. Card recipient must sign in the block. If the recipient is incapable of signing, the condition must be indicated in that block.

Block 73. Date Issued. Enter the date, four-digit year, three alpha-character month, and two-digit day format (YYYYMMMDD), the recipient acknowledged receipt of the ID card. Use nine characters.

Appendix C TASS Email Notifications

I. Schedule for Contractor Reverification Notifications

Reverification Required – Initial Notification – First transmitted 150 days after CAC issued/CAC last verified

Dear {TA},

This message has been sent to notify you that you need to reverify the contractor ({Contractor Name}) requires his/her CAC. Please complete the verification process at the link below.

Questions may be sent via email to: dodhra.dodc-mb.dmdc.mbx.contractor-verification@mail.mil

TASS TA Website: https://www.dmdc.osd.mil/tass

Reverification Timeout Reminder –Transmitted 160 days after CAC issued/CAC last verified

Dear {TA},

This message has been sent to remind you the prescribed time to reverify contractor ({Contractor Name}) has arrived. Please complete the verification process as prescribed.

Questions may be sent via email to: dodhra.dodc-mb.dmdc.mbx.contractor-verification@mail.mil

TASS TA Website: https://www.dmdc.osd.mil/tass

Note this reminder will not be sent if application has been either reverified or revoked.

Reverification Timeout Warning – Transmitted 170 days after CAC issued/CAC last verified

Dear {TA},

This message has been sent to notify you the prescribed time to reverify contractor ({Contractor Name}) has arrived and that that action needs immediate attention. Please complete the verification process as prescribed. The time allotted for you to complete the verification will expire on {Date} at which time the contractor's Defense Enrollment Eligibility Reporting Service record will be terminated.

Questions may be sent via email to: dodhra.dodc-mb.dmdc.mbx.contractor-verification@mail.mil

TASS TA Website: https://www.dmdc.osd.mil/tass

Note this reminder will not be sent if application has been either reverified or revoked.

Reverification Expiration – Transmitted 180 days after CAC issued/CAC last verified

Dear {TA},

The time allotted to reverify contractor {Contractor Name} has expired. As a result, that account has been revoked and the Defense Enrollment Eligibility Reporting System has been updated to reflect the change.

Questions may be sent via email to: dodhra.dodc-mb.dmdc.mbx.contractor-verification@mail.mil

TASS Website: https://www.dmdc.osd.mil/tass

II. Batch Upload Success Notification

Dear {TA},

The Batch File Upload has Finished OK.

Batch execution details:

File Name….: 201201210001.xml

Batch ID….: 201201210001

Successful Count: 3

Error Count….: 0

Total Processed: 3

Execution Start Date/Time: 01/31/2012 15:42:54 Completion Date/Time…:01/31/2012 15:42:59

Questions may be sent via email to: dodhra.dodc-mb.dmdc.mbx.contractor-verification@mail.mil

TASS Web Site: https://www.dmdc.osd.mil/tass/

Appendix D Acronyms, Abbreviations, and Standard Terms

Acronym	Description
BAH	Booz Allen Hamilton
CAC	Common Access Card
CVS	Contractor Verification System
DEERS	Defense Enrollment & Eligibility Reporting System
DMDC	Defense Manpower Data Center
DoD	Department of Defense
DSO	DMDC Support Office
FAQ	Frequently Asked Question
Government Sponsor	Active Duty member or Civil Servant who approves contractor CAC request
ID	Identification
LMS	Learning Management System
LOA	Letter of Authorization
MOA	Memorandum of Agreement
PIN	Personal Identification Number
PIPS	Personnel Identity Protection Solutions
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
POC	Point of Contact
RAPIDS	Real-time Automated Personnel Identification System
SOFA	Status-of-Forces Agreement
SPOC	Service or Agency Point of Contact
SPOT	Synchronized Predeployment & Operational Tracker
SSN	Social Security Number
TA	Trusted Agent
TASM	Trusted Agent Security Manager
TASS	Trusted Associate Sponsorship System
URL	Uniform Resource Locator
USID	Uniformed Services ID
WBT	Web-based Training

Standard TASS Terms	Definition	Example
Account	Refers to the SPOC, TASM, or TA roles in TASS.	For example, a TASM must access his or her TA account to complete TA tasks.
Applicant record	An Applicant's TASS application that has been **approved** or **issued**.	An applicant record can be **reverified**, **reused**, **disabled** or **revoked**.
Application (DD Form 1172-2)	An Applicant TASS application (DD-1172-2 Form) that has **not** completed the full process to approval or issuance, whether in an **in-progress, submitted, disabled, returned, or rejected status**.	For example, An application is created and submitted by a TA and then completed and submitted by an Applicant.
Page	Refers to all webpages **external** to TASS, to include reference to the TASS login and logout pages.	The RAPIDS Site Locator (RSL) webpage at www.dmdc.osd.mil/rsl provides access to the external RSL application.
Role	Refers to the role of an SPOC, TASM, or TA and his or her access in TASS.	For example, only the SPOC role can transfer TAs between sites.
Screen	Refers to all screens a user might navigate to for all **internal** screens within the TASS application.	For example, you can change your work information by clicking the **Edit** link on the 'My Profile' screen.
TASS	The Trusted Associate Sponsorship System web application.	TASS is the DoD official authoritative data source system that allows specified populations to apply for a government credential.
User ID, Username, User Account Code	These are interchangeable terms that refer to the alphanumeric information that is used to log in to TASS or DEERS Security Online.	For example, a TA cannot log in to TASS with a username. However, the TASM will provide the TA with a user account code that is to be kept for reference if the TA needs his or her TASS account reset in Security Online.
Web-Based Training (WBT) Courses	All courses will be titled as Trusted Associate Sponsorship System (TASS) [Role] Training course.	• *TASS Trusted Agent Training* • *TASS Service or Agency Point of Contact Training* • *TASS Trusted Agent Security Manager Training* *TASS Training Overview*

Appendix E Alphanumeric Character Translations

It is important to communicate Applicant's password information clearly and securely. The following translations follow the military standard for communication of alphanumeric data. They will help you to transmit password characters that may be difficult to understand.

Letters	Translation
a	Lower case Alpha
A	Upper case Alpha
b	Lower case Bravo
B	Upper case Bravo
c	Lower case Charlie
C	Upper case Charlie
d	Lower case Delta
D	Upper case Delta
e	Lower case Echo
E	Upper case Echo
f	Lower case Foxtrot
F	Upper case Foxtrot
g	Lower case Golf
G	Upper case Golf
h	Lower case Hotel
H	Upper case Hotel
i	Lower case India
I	Upper case India
j	Lower case Juliett
J	Upper case Juliett
k	Lower case Kilo
K	Upper case Kilo
l	Lower case Lima
L	Upper case Lima
m	Lower case Mike
M	Upper case Mike
n	Lower case November
N	Upper case November
o	Lower case Oscar
O	Upper case Oscar
p	Lower case Papa
P	Upper case Papa
q	Lower case Quebec
Q	Upper case Quebec

r	Lower case Romeo
R	Upper case Romeo
s	Lower case Sierra
S	Upper case Sierra
t	Lower case Tango
T	Upper case Tango
u	Lower case Uniform
U	Upper case Uniform
v	Lower case Victor
V	Upper case Victor
w	Lower case Whiskey
W	Upper case Whiskey
x	Lower case X-ray
X	Upper case X-ray
y	Lower case Yankee
Y	Upper case Yankee
z	Lower case Zulu
Z	Upper case Zulu

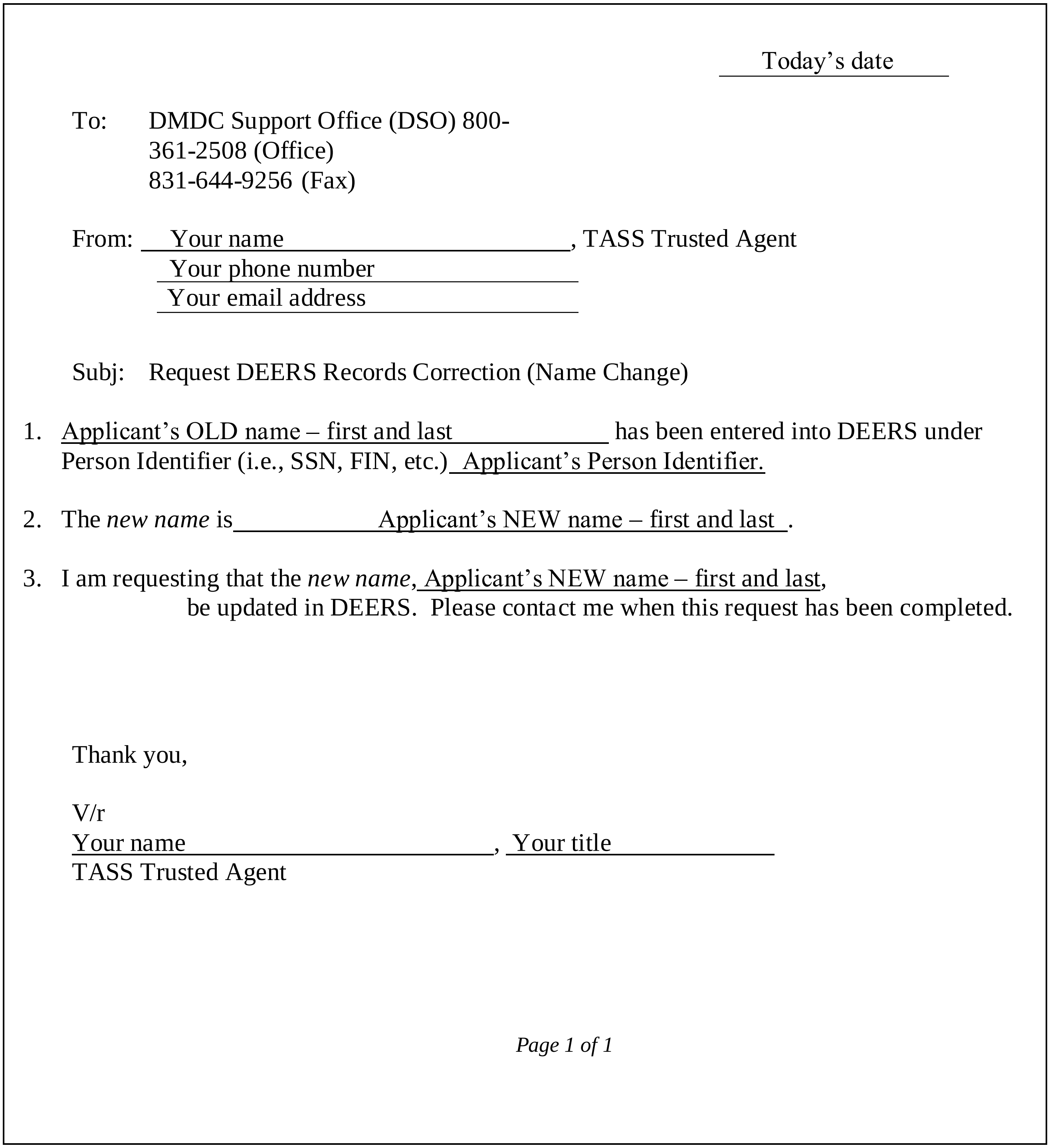
Numbers	**Translation**
1	Number One
2	Number Two
3	Number Three
4	Number Four
5	Number Five
6	Number Six
7	Number Seven
8	Number Eight
9	Number Nine
0	Number Zero

Special Characters	**Translation**
(	Left parenthesis
)	Right parenthesis
-	Dash
!	Exclamation Point
<	Left carat or Less-than sign
>	Right carat or More-than sign

#	Pound sign or Hash mark
$	Dollar sign
%	Percent sign
&	Ampersand sign
*	Asterisk or Star
?	Question mark

Appendix F Documentation for DEERS Data Changes

I. DSO Name Correction Request Form



Today's date

To: DMDC Support Office (DSO) 800-
361-2508 (Office)
831-644-9256 (Fax)

From: Your name , TASS Trusted Agent
Your phone number
Your email address

Subj: Request DEERS Records Correction (Name Change)

1. Applicant's OLD name – first and last has been entered into DEERS under Person Identifier (i.e., SSN, FIN, etc.) Applicant's Person Identifier.

2. The *new name* is Applicant's NEW name – first and last .

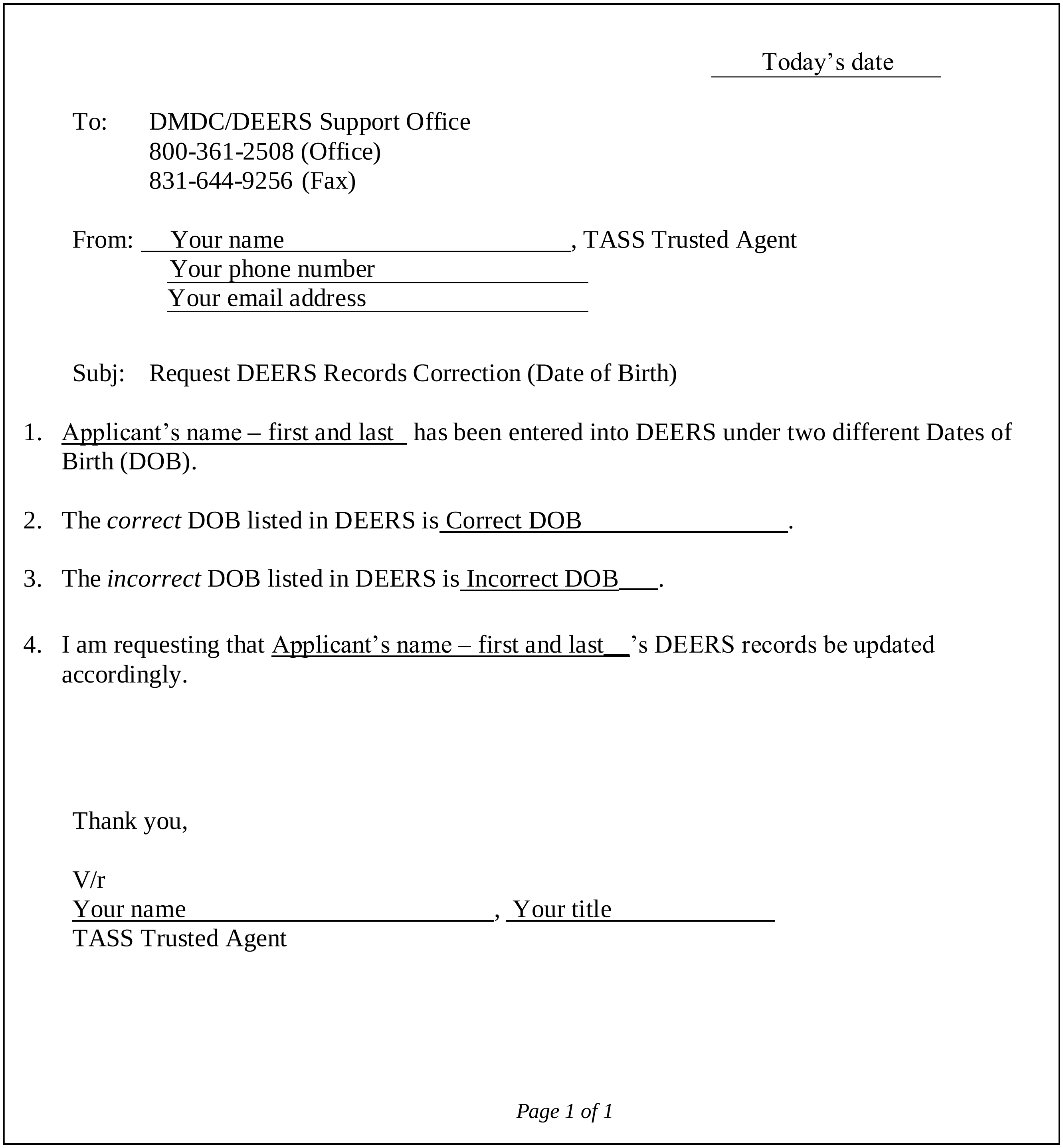
3. I am requesting that the *new name*, Applicant's NEW name – first and last, be updated in DEERS. Please contact me when this request has been completed.

Thank you,

V/r
Your name , Your title
TASS Trusted Agent

Page 1 of 1

II. DSO DOB Correction Request Form



Today's date

To: DMDC/DEERS Support Office
800-361-2508 (Office)
831-644-9256 (Fax)

From: Your name, TASS Trusted Agent
Your phone number
Your email address

Subj: Request DEERS Records Correction (Date of Birth)

1. Applicant's name – first and last has been entered into DEERS under two different Dates of Birth (DOB).

2. The *correct* DOB listed in DEERS is Correct DOB.

3. The *incorrect* DOB listed in DEERS is Incorrect DOB.

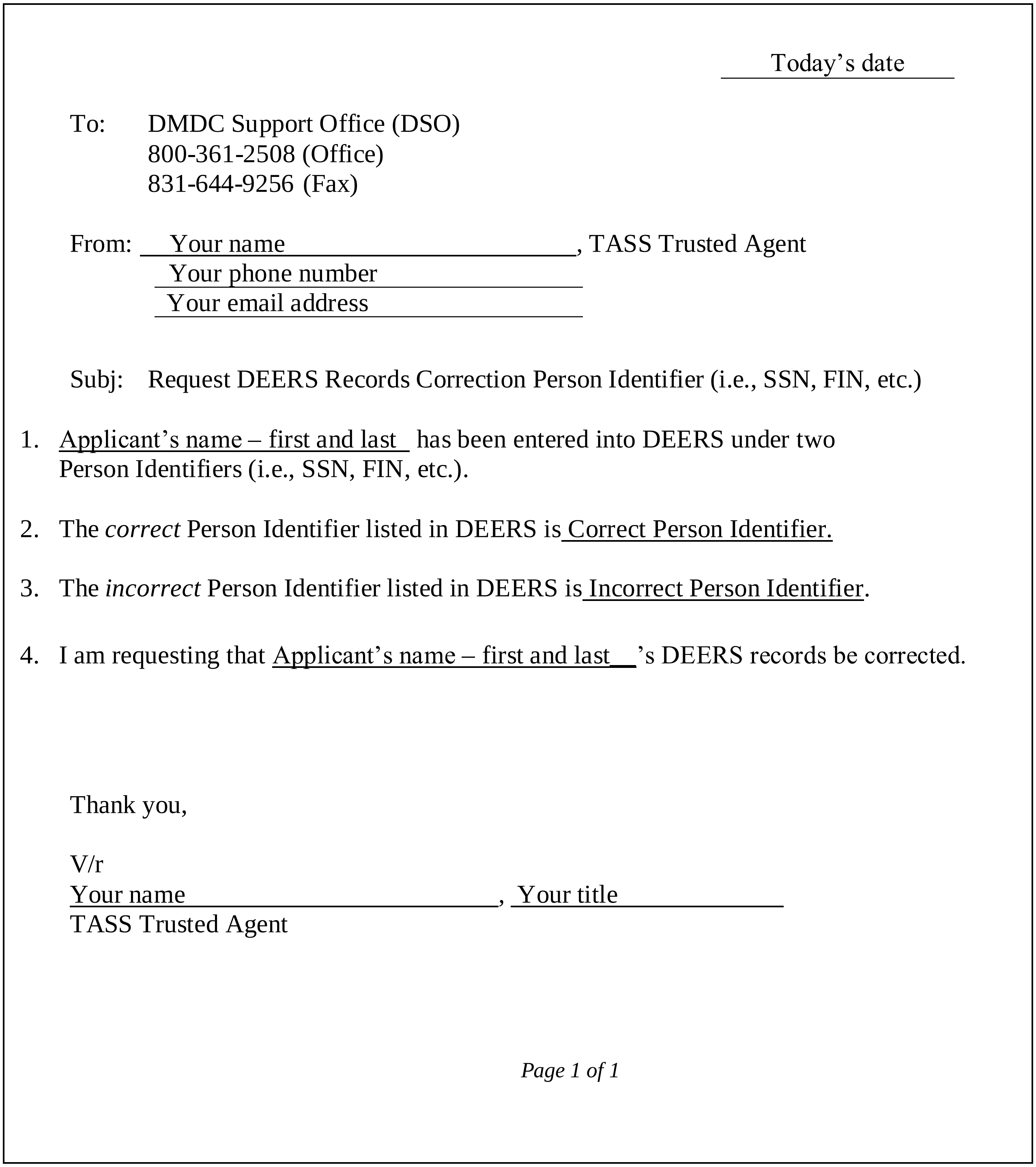
4. I am requesting that Applicant's name – first and last's DEERS records be updated accordingly.

Thank you,

V/r
Your name, Your title
TASS Trusted Agent

Page 1 of 1

III. DSO Person Identifier Correction Request Form



Today's date

To: DMDC Support Office (DSO)
800-361-2508 (Office)
831-644-9256 (Fax)

From: Your name, TASS Trusted Agent
Your phone number
Your email address

Subj: Request DEERS Records Correction Person Identifier (i.e., SSN, FIN, etc.)

1. Applicant's name – first and last has been entered into DEERS under two Person Identifiers (i.e., SSN, FIN, etc.).
2. The *correct* Person Identifier listed in DEERS is Correct Person Identifier.
3. The *incorrect* Person Identifier listed in DEERS is Incorrect Person Identifier.
4. I am requesting that Applicant's name – first and last's DEERS records be corrected.

Thank you,

V/r
Your name, Your title
TASS Trusted Agent

Page 1 of 1